Departamento de Informática
Ingeniería Técnica en Informática de Gestión

PROYECTO FIN DE CARRERA

AUDITORÍA DE LA SEGURIDAD Y EL CONTROL EN DISPOSITIVOS MÓVILES

Autor: Alicia Verdúguez Merín.

Tutor: Miguel Ángel Ramos González.

Leganés, octubre de 2015

Título: AUDITORÍA DE LA SEGURIDAD Y EL CONTROL EN DISPOSITIVOS MÓVILES
Autor: ALICIA VERDÚGUEZ MERÍN
Director: MIGUEL ÁNGEL RAMOS GONZÁLEZ

EL TRIBUNAL

Presidente: _____

Vocal: _____

Secretario: _____

Realizado el acto de defensa y lectura del Proyecto Fin de Carrera el día __ de _____ de 20__ en Leganés, en la Escuela Politécnica Superior de la Universidad Carlos III de Madrid, acuerda otorgarle la CALIFICACIÓN de

VOCAL

SECRETARIO PRESIDENTE

Agradecimientos

A mi tutor Miguel Ángel, por haber estado dispuesto a ayudarme a terminar lo empezado hace ya bastante tiempo, por su dedicación, por su colaboración, por su profesionalidad. Gracias.

A mis padres, por haberme dado siempre aliento y haber estado pendientes de este PFC. Sin vosotros se hubiese quedado sin terminar.

A José Antonio, por todo, por estar ahí, por convertir los días malos en días buenos por haberme sabido escuchar y apoyar en todo momento. Por todo lo vivido y sobre todo por hacerme feliz.

A Inés, por regalarme cada mañana esa sonrisa que ha sido mi inspiración para seguir adelante en esta contrareloj.

Muchas gracias a todos.

Resumen

El presente documento tiene por objetivo reflejar una completa visión sobre como de importante es la seguridad informática en los dispositivos, tanto a nivel particular como a nivel profesional, mostrar por qué es necesaria y dar a conocer qué es lo que debemos proteger y cómo hacerlo.

Además, en paralelo, también se mostrará el prototipo de una aplicación que serviría para evaluar la seguridad existente en un determinado dispositivo o aplicación.

Abstract

The present document aims to reflect a full vision about how is highlighted the informatic security in the mobile device, as a particular level as a professional level, to show why is necessary and to publish what is what we must protect and how protect it.

In addition, concurrently, the prototype of an application will be showed also. It would be used for assessing the existence security in a certain mobile device or application.

Índice general

Índice de figuras

Índice de tablas

Capítulo 1

Introducción y objetivos

1.1 Introducción

Los dispositivos móviles constituyen uno de los principales, si no el principal, medio de comunicación que utilizamos en la actualidad. Cada vez son utilizados por más personas, y cada vez se emplean en un mayor número de escenarios y ámbitos diferentes, desde el ocio personal, hasta el acceso a datos corporativos de una organización o empresa con un alto nivel de confidencialidad, pasando por multitud de aplicaciones de uso cotidiano, como el acceso al correo electrónico, a las redes sociales, a la navegación por internet etc.

Se considera dispositivo móvil aquél dispositivo de uso personal o profesional de reducido tamaño que permite la gestión de información y el acceso a redes de comunicaciones, tanto de voz como de datos, y que habitualmente dispone de capacidades de telefonía, como por ejemplo teléfonos móviles, smartphones (teléfonos móviles avanzados o inteligentes) y agendas electrónicas (PDA), independientemente de sí disponen de teclado o pantalla táctil.

En líneas generales, los dispositivos móviles comprendidos en el ámbito de aplicación de este trabajo poseen las siguientes características comunes:

- Tamaño reducido.
- Interfaz inalámbrico para acceso remoto y comunicación de datos.
- Memoria interna, no removible.

- Sistema operativo, en general distinto a los usados en ordenadores de sobremesa y portátiles.
- Una o varias cámaras digitales.
- Micrófono.
- Interfaces para la conexión de memorias externas.
- Mecanismos para sincronizar la información local del dispositivo con otros equipamientos.

A lo largo de este proyecto fin de carrera se hablará de lo importante que es mantener un nivel de seguridad alto en los dispositivos, se explicará que es un dato personal y lo preciados que pueden llegar a ser para los ciberdelicuentes, las amenazas a las que están expuestos, las pautas mínimas que deben cumplirse a nivel particular y las que están obligadas a cumplir a nivel profesional las entidades, organizaciones o empresas que puedan manejar algún tipo de dato personal.

1.2 Objetivos

Los objetivos de este proyecto fin de carrera son, como ya hemos adelantado, los siguientes:

- **Divulgación de la importancia de la seguridad informática**: Pues es la parte menos conocida de la carrera. Mi interés por ella apareció al cursar las asignaturas de Auditoría informática y Gestión de la calidad con Miguel Ángel Ramos, al no tratarse de asignaturas obligatorias pasan muchas veces desapercibidas y hacen que muchos alumnos concluyan sus estudios en informática sin conocer esta rama.
- **Devolver la importancia a la privacidad:** Los nuevos tiempos hacen que la privacidad este pasando a un segundo plano sin apenas darnos cuenta. Con este proyecto se pretende que el lector comprenda su importancia. De forma particular el usuario debe conocer sus derechos gracias a la LOPD y las pautas a tomar para poder salvaguardar sus datos al conocer también lo vulnerable que puede llegar a ser. A nivel general se explicará como la ley obliga a las entidades a proteger los datos en sus sistemas de información, como para ello las audita e incluso las repercusiones que tendría un problema en la privacidad de una entidad tanto a nivel de imagen como económico.

1.3 Estructura de la memoria

Para facilitar la lectura de la memoria, se incluye a continuación un breve resumen de cada capítulo.

- Capitulo 2 - **LA SEGURIDAD**: En él se muestra el concepto de seguridad de la información y de seguridad Informática,
- Capítulo 3 - **POR QUE ES NECESARIA LA SEGURIDAD**: Se verán los distintos estados de la Información a proteger y las formas de hacerlo
- Capítulo 4 - **¿QUÉ PROTEGER? DATOS PERSONALES**: Se reflejan los distintos datos que se deben proteger, cuan de importantes son y las pautas básicas para hacerlo.
- Capítulo 5 - **AMENAZAS DE SEGURIDAD EN LOS DISPOSITIVOS MOVILES**: Se lleva a cabo un recorrido enumerando las distintas amenazas de seguridad en los dispositivos móviles que han ido surgiendo en los últimos tiempos.
- Capítulo 6 - **¿CÓMO PREVENIR? MECANISMOS DE SEGURIDAD:** En este capítulo se recogen las medidas de seguridad recomendadas para un sistema seguro.
- Capítulo 7 – **ORGANISMOS. IMPLANTACIÓN DE LA SEGURIDAD DE LOS DISPOSTIVOS MOVILES:** Breve recopilación de la implantación de un método de seguridad en una organización.
- Capítulo 8 – **AUDITORÍA DE SEGURIDAD INFORMÁTICA:** Este capítulo esta dedicado a la explicación de cómo debe ser una auditoría, los tipos de auditoría que existen, por que es importante realizarlas etc.
- Capítulo 9 – **LEGISLACIÓN ACTUAL EN ESPAÑA:** Se trata de la recopilación de la legislación referente a la seguridad informática existente en España.
- Capítulo 10 – **DESARROLLO DE LA APLICACIÓN:** En este capítulo se desarrolla un prototipo de una aplicación pensada para analizar la seguridad de un dispositivo / aplicación / sistema etc.
- Capítulo 11 – **GESTION DEL PROYECTO:** Capítulo donde se muestra la estimación inicial del proyecto, la planificación real y un análisis de la misma, así como la enumeración de los recursos empleados.
- Capítulo 12 – **CONCLUSIONES FINALES:** Recopilación de conclusiones una vez terminando el proyecto fin de carrera.

Capítulo 2

La seguridad

Con respecto a la palabra a tratar en esta memoria "SEGURIDAD", existen diversas connotaciones y definiciones:

- Según la **RAE**: "*Cualidad de seguro o la calidad de estar libre y a cubierto de todo riesgo*".
- Según la **Wikipedia**: "*Cotidianamente se puede referir a la seguridad como la ausencia de riesgo o también a la confianza en algo o alguien*".

Es buscando en portales más específicos, donde comenzamos a encontrar la vertiente de SEGURIDAD que buscamos para orientar este proyecto, es decir, la asociada al concepto de protección de información

- Según **Alegsa** (un portal de Internet, informática y tecnologías de la información) se define la seguridad cómo: "*La seguridad informática es una disciplina que se relaciona a diversas técnicas, aplicaciones y dispositivos encargados de asegurar la integridad y privacidad de la información de un sistema informático y sus usuarios*." [ALEG]
- El estándar internacional **ISO27002** nos da otra definición de lo que podemos entender por seguridad de la información: "*La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales*."

La importancia de la seguridad de la información es un elemento de significante y creciente preocupación en las organizaciones modernas, hasta el punto de constituir un

activo altamente apreciable que puede llegar a crear la diferencia entre el éxito y el fracaso de una organización.

Ligado al término “Seguridad de la Información” surge “Seguridad Informática”, ambos persiguen una misma finalidad, proteger la información de un rango amplio de amenazas, pero su significado no es el mismo.

2.1 Concepto de Seguridad de la Información

La **seguridad de la información** es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma. {WIKIPEDIA} independientemente de la forma en que se dispongan los datos: electrónicos, impresos, audio, etc.

El campo de la Seguridad de la Información ha crecido y evolucionado considerablemente en los últimos años. Convirtiéndose en una carrera acreditada a nivel mundial. La misma ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital o administración de sistemas de gestión de seguridad por nombrar algunos.

La correcta Gestión de la Seguridad de la Información busca establecer y mantener programas, controles y políticas, que tengan como finalidad conservar los principios comentados “confidencialidad”, “integridad” y “disponibilidad” de la información”.

- **CONFIDENCIALIDAD:**

La confidencialidad es la propiedad por la que se garantiza que la información está accesible únicamente a personal autorizado a acceder a dicha información. La confidencialidad ha sido definida por la Organización Internacional de Estandarización (ISO) en la norma ISO/IEC 27002 como “garantizar que la información es accesible sólo para aquellos autorizados a tener acceso” [ISO27002]

Es a raíz de este principio donde aparece el término de la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros. Esto debe hacerse siempre en un sistema que garantice la confidencialidad, es decir, garantizando que si un tercero entra en posesión de la información intercambiada entre remitente y el destinatario no es capaz de extraer ningún contenido inteligible. Para garantizarla se utilizan mecanismos de cifrado y de ocultación de la comunicación. Por ejemplo, digitalmente se puede mantener la confidencialidad de un documento con el uso de “claves asimétricas”. Los mecanismos de estos cifrados garantizan la confidencialidad durante el tiempo necesario para descifrar el mensaje. Por esta razón es necesario determinar durante cuánto tiempo el mensaje debe seguir siendo confidencial. Pero es importante tener siempre en cuenta que a día de hoy no existe ningún mecanismo de seguridad absolutamente seguro.

- **INTEGRIDAD:**

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas. Pues hay amenazas a la seguridad que no sólo se encargan de destruir la información, muchas veces alterar dichos datos haciendo que tomen un valor incorrecto puede ser más dañino que su mera destrucción.

- **DISPONIBILIDAD:**

Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

2.2 Concepto de Seguridad Informática

La seguridad informática es área de la informática cuyo objetivo radica en la protección de la información y de los sistemas de la información, tanto en el acceso a ellos, en el uso, en la divulgación, en la modificación, o en la destrucción de la información. Para llevar a cabo la mencionada tarea existen unas determinadas pautas, recogidas como estándares, protocolos o incluso leyes que han sido desarrolladas para minimizar los posibles riesgos que afecten a la infraestructura o a la información contenida en los sistemas.

La seguridad informática comprende tanto la parte lógica como la física así como todo lo que signifique un riesgo para la organización, entidad o incluso para un usuario de a pie si la información llegase a manos de otras personas.

Así pues, está concebida para proteger los activos informáticos, entre los que se encuentran los siguientes:

- **La infraestructura computacional**: Se trata de la columna vertebral de la organización, pues es importante tanto para el almacenamiento y gestión de la información, como para el funcionamiento de la organización. La seguridad informática tiene como misión en esta área custodiar los equipos, hacer que estos funcionen adecuadamente, anticiparse con medias de prevención a cualquier tipo de fallo como puede ser un robo, un incendio, un desastre natural etc. e incluso paliar en la medida de lo posible las consecuencias mediante planes de acción previstos en caso de que estos fallos se consumaran.

- **Los usuarios**: Son las personas que utilizan la estructura tecnológica, y que gestionan o manejan la información. Debe protegerse el sistema de tal manera que un uso no adecuado por parte de ellos no sea capaz de poner en entredicho la seguridad de la información.

- **La información**: es el activo más importante pues utiliza y reside en la infraestructura computacional y es utilizada por los usuarios.

Capítulo 3

¿Por qué es necesaria la seguridad?

Actualmente, uno de los activos más preciados es la información, tanto para una empresa u organización como a nivel personal. Si además se trata de información sensible o confidencial su revelación, alteración, perdida o destrucción puede producir daños importantes. Es por ello que surge la misión de proteger dicha información.

Como ya hemos oído o leído en multitud de ocasiones, la pérdida de información sensible puede producirse accidental o malintencionadamente, pero, en cualquier caso, puede y suele acarrear un daño económico y de prestigio, afectando a la empresa y su marca asociada.

Es más sencillo de lo que parece perder información sensible o dejarla expuesta a diferentes riesgos y amenazas, por ejemplo mediante el envío de algún correo electrónico a un destinatario erróneo, esta equivocación realmente no es demasiado inusual en personas que utilicen de forma intensiva el correo electrónico, aunque sea enviando información poco relevante, pero, ¿Qué sucedería si la información enviada en ese correo electrónico fuese confidencial para la empresa?, ¿Y si la transmisión de esa información sin el consentimiento del propietario de la misma estuviera incumpliendo alguna ley? Pues probablemente tendríamos un serio problema, bien porque dicha información confidencial pudiera caer en manos de nuestra competencia o porque el descuido nos enfrentara a una multa económica por el incumplimiento de alguna ley.

Pero no hace falta basarnos en la información confidencial que pueda querer protegerse en una empresa, con un simple vistazo sobre la realidad diaria podemos ver cómo cada vez disponemos de más canales por los que es necesario gestionar y transferir correctamente la información. Algunos ejemplos muy recientes de ello son las redes

sociales o los dispositivos móviles. A día de hoy la información que circula por estos canales es exagerada, (según google en 2014 Facebook compartió más de 10 millones de fotografías cada día o en el caso de YouTube se subió una hora de vídeo cada segundo) y no guarda ningún tipo de proporción con las medidas de protección o monitorización existentes en estos campos a día de hoy, por lo que el en la seguridad de la Información aún existe un gran vacío.

3.1 Estados de la Información a proteger

Para ello, es muy importante tener claro los distintos estados de la información en función de su ubicación:

- **Información en reposo**: Son todos aquellos datos que residen en los sistemas de archivos, bases de datos y cualquier otro medio de almacenamiento tradicional y normalmente alojados en los centros de datos de las empresas.
- **Información en tránsito**: Se trata de los datos que se mueven hacia el exterior de la empresa a través de redes públicas, habitualmente Internet.
- **Información en el punto final (endpoint)**: Se trata de datos almacenados en los terminales de los usuarios o en dispositivos de almacenamiento portables (por ejemplo: USB, CD o DVD, discos duros externos, reproductores MP3, portátiles o smartphones).

3.2 Formas de proteger la información

Para tratar de evitar la pérdida de información sensible, debemos identificar qué información es realmente vital para la empresa, entidad o persona, antes de poder protegerla adecuadamente. Evidentemente, esta tarea no es sencilla y requiere un estudio pormenorizado en cada caso, pero siempre existe una base inicial sobre la que empezar a trabajar, como son el cumplimiento regulatorio o la protección de propiedad intelectual.

En el caso de empresas u organizaciones, suele ser responsabilidad de la alta dirección preservar la seguridad e integridad del sistema de información ya que la estructura de datos de la empresa es un fiel reflejo de la actividad de negocio de la misma, viene además especificado en el Artículo 79, del Título VIII, del Real Decreto 172072007 " *Los responsables de los tratamientos o los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad con arreglo a lo dispuesto en este Título, con independencia de cual sea su sistema de tratamiento*". [RD1720]

A la hora de hablar de protección de información, saltan a la palestra diversas tecnologías basadas tanto en proteger las fugas de información mediante controles de los repositorios y medios de transmisión como muchas otras centradas en el control de

acceso y uso de los archivos a proteger independientemente del lugar en que se encuentren.

Para las primeras, Data Loss Prevention DLP, tal como su propio nombre indica, su principal reto debe ser facilitar el trabajo de prevención y detección de fugas de información. Para ello, deben ser capaces de identificar, proteger y supervisar las acciones llevadas a cabo sobre la información sensible o confidencial. Estas capacidades debe realizarlas sobre los distintos estados de la información (almacenada, en tránsito o en el punto final o endpoint).

En cuanto a los EDRM (Enterprise Data Right Management) o IRM (Information Rights Management), su principal misión es la protección de los derechos digitales, tanto de usuarios externos como internos a la organización, con independencia del lugar en el que se encuentre la información. Al no importar la ubicación de ésta, deben disponer de mecanismos de autenticación suficientemente robustos e interoperables con el resto de soluciones de la organización.

El uso de estas tecnologías debe ayudarnos a proteger la privacidad de los datos, la propiedad intelectual y el cumplimiento normativo, permitiendo en todo momento advertir sobre el acceso a información protegida y, en caso necesario, el bloqueo de las acciones realizadas, si existe incumplimiento de la política de seguridad de la empresa o de los derechos digitales.

Puesto que ambas tecnologías presentan puntos fuertes y débiles y que, desde una perspectiva empresarial, la protección de la información sensible debe tener un enfoque global, todo hace indicar que son tecnologías condenadas a entenderse y complementarse.

Pero una vez más, llegamos a la conclusión de que la Seguridad de la Información es un proceso en el que debemos combinar distintas medidas de seguridad para conseguir nuestro objetivo. A pesar de las bondades de las tecnologías DLP y EDRM o IRM, éstas no pueden cumplir su cometido si no tenemos en cuenta otros aspectos fundamentales como por ejemplo disponer de una política de Seguridad de la Información, es decir, contar con un sistema de identificación para la información específica que debe protegerse, incluyendo las revisiones periódicas, que lo mantengan lo más actualizado posible. Esto consiste en mantener procedimientos para la protección y el control de la información protegida, de modo que sólo sea accesible por aquéllos que tienen la necesidad de conocerla, trasladándole el deber de protegerla. Dicho deber, en algunas circunstancias, puede ser impuesto por Ley, pero, en cualquier caso, debe establecerse en la empresa como parte del acuerdo de confidencialidad con el empleado.

Un sistema de alerta y aviso que advierta sobre la sensibilidad de la información y los requisitos establecidos para el manejo de la misma. Habitualmente, ésta es una de las funcionalidades del DLP, pero, de todas formas, es importante que el usuario sepa que está accediendo a información sensible y cómo debe actuar durante el tratamiento de la misma.

Por tanto, y puesto que no es muy recomendable empezar la casa por el tejado, lo que realmente tendremos que hacer es una correcta gestión de la seguridad de nuestra información. Para ello, debemos apoyarnos en las normativas y buenas prácticas existentes, como las normas ISO 27001 y 27002, y, por supuesto, en las distintas soluciones tecnológicas que nos ayuden a cumplir nuestro objetivo final, que no es otro que proteger la información sensible en cualquier formato, evitando un posible mal uso de la misma o su extravío, ya sea de una manera accidental o intencionada.

Capítulo 4

¿Qué proteger? Datos personales

Es probable que la mayoría de los usuarios no sean conscientes de la gran cantidad de información existente en la red sobre ellos. En muchas ocasiones esa información es, incluso, proporcionada por ellos mismos ignorando que permanecerá en internet, accesible para quien quiera buscarla, durante mucho tiempo.

Vivimos conectados, diariamente se publican miles de datos que en un instante pasan a estar disponibles en todo el mundo dejando así una huella muy difícil de borrar. Este rastro es la identidad digital y está compuesto tanto por los datos que publicamos de forma consciente como por la información que se recopila sin que nos demos cuenta.

Es importante darle a nuestra información el valor que tiene, diariamente, en la sociedad en la que vivimos se nos solicita información para cualquier tipo de actividad (reservar un vuelo, comprar entradas, pedir información sobre una tienda online, etc. Facilitamos datos como el DNI, el nombre, los apellidos, el teléfono, el correo electrónico sin pensar que lo que estamos dando es una información muy valiosa, pues ese conjunto de datos permite identificar a una persona, debemos ser cautelosos y al igual que no dejaríamos un albún fotográfico en un vagón del metro, deberíamos ser igual de cuidadosos con nuestras publicaciones en blogs, redes sociales, etc… pues muchas de ellas (fotos, mensajes en redes sociales, publicaciones) permiten identificar total o parcialmente a una persona y cuanta más información sepa un ciberdelincuente de nosotros más fácil se lo ponemos.

A toda esa información denominada DATOS PERSONALES es a la que encaminaremos todas las medidas de protección.

Es importante conocer los riesgos de hacer públicos ciertos datos:

- **Correo electrónico.** Que nuestro correo deje de ser privado hará que comencemos a recibir cada vez mayor número de spam, mensajes con intentos de engaño (phishing), fraude, etc.
- **Datos bancarios.** Facilitar nuestros datos bancarios nos puede exponer a una pérdida económica. Seamos muy precavidos con las páginas web donde utilizamos estos datos para realizar compras online y nunca facilitemos este tipo de datos por correo electrónico. En 2012 y 2013 fue muy común en España el virus de la Policía. Éste alertaba al usuario que era culpable de algún delito y pedía el pago de una multa de 100 euros. El mensaje incluía el logo de la Policía Nacional y en ocasiones la fotografía del propio usuario, capturada con la webcam.
- **Ubicación geográfica.** Publicar los lugares que solemos frecuentar proporciona información que permite que alguien malintencionado pueda tanto conocer nuestra rutina o hábitos diarios e incluso saber cuando nos encontramos fuera de casa, como localizarnos en persona.
- **Fotos y vídeos.** Nuestras fotografías y vídeos personales contienen mucha más información de la que pensamos: en ellas se haya implícito ubicaciones físicas, quiénes son nuestros amigos y familiares, cuál es nuestro nivel económico, qué aspecto tiene nuestro domicilio, gustos, preferencias, etc.

4.1 Datos de Navegación

A la hora de navegar por la red también debemos ser cautelosos, pues involuntariamente proporcionamos información. El navegador que utilicemos almacena datos como el historial de páginas que visitamos, contraseña que utilizamos, datos introducidos en formularios, cookies de navegación etc. (En el caso de las cookies de navegación la legislación española impide que las páginas webs las instalen en nuestros dispositivos a menos que hayamos dado un consentimiento expreso para ello.

Dado que todos estos datos mencionados aportan mucha información sobre nosotros, existen determinados programas diseñados para robarla y cederla a ciberdelincuentes. Es por ello conveniente que configuremos nuestro navegador para que no los almacene o en caso contrario que periódicamente borremos estos datos.

4.2 Registro en servicios online

Siempre que queremos registrarnos en algunos servicios se nos piden nuestros datos personales (nombre, apellidos, fecha de nacimiento, DNI, correo electrónico, teléfono), en muchas ocasiones el usuario no puede controlar con exactitud a quien van dirigidos finalmente estos datos, ni quien va a acceder a ellos, ni con qué fin. La ley

española obliga a las empresas a mantener en secreto estos datos pero a muchas de ellas no les aplican estas medidas por residir en otros países.

Es importante por este motivo, valorar antes de darnos de alta en algún servicio, qué datos nos piden y qué uso van a hacer de ellos. Para ello debemos leer las condiciones de uso y la política de privacidad del servicio antes de facilitar cualquiera de nuestros datos.

4.3 Dispositivos móviles

Otro riesgo se encuentra en que los dispositivos móviles como tabletas, smartphones, portátiles suelen almacenar gran cantidad de información privada como fotos personales, videos, contactos, acceso a redes sociales, datos de pago para compras online. Si alguien accede a toda esta información conocerá gran parte de nuestra vida en incluso podrá suplantar nuestra identidad realizando por ejemplo compras por internet.

Es por ello que debemos proteger la información que almacenamos en ellos, estableciendo modos de acceso seguro mediante contraseñas o patrones de pantalla. O utilizar aplicaciones que permiten el bloqueo y el borrado de datos en remoto, que protegen nuestra información en caso de extravío del dispositivo.

4.4 Lugares y equipos públicos

A veces para conectarnos a internet utilizamos equipos ajenos, o nos conectamos en lugares como aeropuertos, hoteles, donde nos ofrecen WiFi abierta de forma gratuita. En estos casos es recomendable evitar el envío de información personal, pues puede que si el dispositivo no es nuestro no conozcamos el nivel de protección del que dispone, que nuestros datos se queden grabados en él, o que no muy lejos de nosotros conectado a la misma red tengamos a algún ciberdelicuente capaz de capturar lo que estamos enviando a la red, incluso las contraseñas.

4.5 Pautas básicas a tener en cuenta

Como ya hemos comentado, todo lo que hacemos en Internet deja un rastro y nuestra información personal no solo es valiosa para nosotros, lo es también para los ciberdelincuentes. Siguiendo algunos consejos básicos podremos incrementar la seguridad de nuestra información en la red:

- **Ser cuidadoso con la información que se publica.** Una vez publicada en Internet, ésta es casi permanente, escapa de nuestro control y es accesible desde cualquier lugar del mundo.

- **Configuración adecuada de la privacidad en las redes sociales.** Todas ellas ofrecen opciones de privacidad para que controlemos quién tiene acceso a las publicaciones.
- **Conocer nuestros derechos.** La ley de protección de datos obliga a todas las empresas españolas a proteger y a mantener en secreto los datos de sus clientes, sin embargo no a todas las empresas les aplica esta ley por residir en otros países. Infórmate, lee las condiciones de privacidad y haz valer tus derechos.
- **Ser precavido con los dispositivos y los lugares públicos.** No se ha de olvidar la seguridad en los dispositivos, y utilizar siempre redes seguras para compartir información.
- **Solicita a Google o a otros buscadores la retirada de información publicada sobre ti que te pueda estar perjudicando.** Existe el derecho al olvido.

Capítulo 5

Amenazas de Seguridad en los Dispositivos Móviles

En este capítulo se detallan las numerosas amenazas y vulnerabilidades asociadas a los dispositivos. Impactos que ponen en riesgo la seguridad tanto del propio dispositivo como de la información que gestiona.

Estos riesgos de seguridad asociados a los dispositivos móviles son múltiples, desde la pérdida o robo del dispositivo (afectando a su disponibilidad), hasta la obtención de la información almacenada y enviada o recibida por el dispositivo (afectando a su confidencialidad), pasando por la suplantación del propietario del dispositivo, lo que afectaría a su integridad.

5.1 Acceso físico al dispositivo móvil

La amenaza de acceso físico a un dispositivo móvil por parte de actores maliciosos, incluso por un breve periodo de tiempo, sigue siendo uno de los vectores de ataque principales que posee habitualmente un doble objetivo, acceder a los datos contenidos en el propio dispositivo, así como encontrar una vía libre para proceder a la instalación de software de espionaje encubierto o malicioso.

Debido a su tamaño y portabilidad estos dispositivos pueden usarse en ubicaciones muy diversas siendo este su mayor atractivo y a la vez uno de los mayores

problemas que plantea la securización de los dispositivos móviles, obligando así a considerar incidentes tales como el extravío o el hurto de forma permanente, ya que podría conllevar pérdidas económicas notables asociadas al valor propio del terminal y de la información que este contiene o a la que se pueda acceder remotamente.

Existe software comercial de espionaje, orientado inicialmente a la monitorización de terminales, pero que puede igualmente ser utilizado por un atacante con fines fraudulentos o delictivos. Este tipo de software permite por ejemplo acceder a la lista de llamadas y mensajes de texto enviados y recibidos, recibir notificaciones cuando éstas tienen lugar o cuando el teléfono se enciende, interceptar las llamadas, recibir notificaciones de la localización de la víctima, etc. Este software permanece oculto en el dispositivo, indetectable, realizando la función para la que ha sido diseñado. Además la instalación de software espía no siempre requiere acceso físico al dispositivo, sino que puede llevarse a cabo a través de actualizaciones remotas, tal como sucedió a los usuarios de BlackBerry en los Emiratos Árabes Unidos al recibir una mejora de software por parte de la operadora Etisalat. Ésta, en lugar de mejorar el rendimiento del dispositivo como prometía, permitía la monitorización de los mensajes de los usuarios. El acceso al dispositivo y a su información está protegido habitualmente por contraseñas simples como el PIN o código de acceso. Desafortunadamente, estos códigos poseen cuatro dígitos, que potencialmente pueden ser fácilmente adivinables o utilizan valores por defecto conocidos, como 0000 ó 1234.

A continuación se incluyen las medidas de Seguridad recomendadas por el ENS para garantizar el control de acceso en los dispositivos móviles.

OP.ACC	CONTROL DE ACCESO	
op.acc.1	Identificación	Necesidad de disponer de mecanismos de identificación de: a) Usuarios de dispositivos móviles. b) Los propios dispositivos.
op.acc.2	Requisitos de acceso	Determinación de los Niveles de Acceso fijados por el organismo, en relación con los recursos corporativos a los que puede accederse a través de dispositivos móviles.
op.acc.4	Proceso de gestión de derechos de acceso	Atendiendo a: mínimo privilegio, necesidad de conocer y capacidad de autorizar.
op.acc.5	Mecanismo de autenticación	Atendiendo al nivel des sistema.
op.acc.6	Acceso local	Se considera acceso local el realizado desde los dispositivos móviles a los recursos corporativos desde dentro de las propias instalaciones de la organización y utilizando redes controladas por el organismo.
op.acc.7	Acceso Remoto	Se considera acceso remoto el realizado desde los dispositivos móviles ubicados fuera de las propias instalaciones de la organización, a través de redes de terceros (en general, a través de internet público o redes de telefonía móvil).

Tabla 1. Medidas de seguridad recomendadas por el ENS para garantizar el control de acceso en los dispositivos móviles.

5.2 Sistema operativo del dispositivo móvil

Es otro de los frentes a cubrir, todos los fabricantes del sistema operativo que gobierna los dispositivos móviles, como Windows Mobile, iPhone o Android, publican periódicamente vulnerabilidades de seguridad asociadas a los componentes y librerías básicas del sistema, con el objetivo de que el dispositivo en cuestión sea actualizado con

las últimas medidas de seguridad desarrolladas, ya que de no ser así el dispositivo estará expuesto a vulnerabilidades públicamente conocidas tanto locales como remotas. Este tipo de vulnerabilidades han sido empleadas en el pasado por atacantes y malware para disponer de acceso completo al dispositivo mediante la ejecución de código, la realización de ataques de denegación de servicio, o el robo de información.

A continuación se muestran algunos enlaces a las alertas y a las actualizaciones de seguridad de los principales fabricantes de los sistemas operativos disponibles en los dispositivos móviles:

- Microsoft Windows Mobile security updates:
  http://www.microsoft.com/windowsmobile/en-us/help/security/updates.mspx
- Android Security Announcements:
  http://groups.google.com/group/android-security-announce
- Apple security updates:
  http://support.apple.com/kb/ht1222
- Palm WebOS software update information:
  http://kb.palm.com/wps/portal/kb/common/article/22767_en.html

Desafortunadamente, los recursos que publican las actualizaciones de seguridad de algunos fabricantes son difíciles de localizar, proporcionan un número reducido de actualizaciones, y/o limitan los detalles de las vulnerabilidades existentes.

5.3 Almacenamiento de Información

A día de hoy los dispositivos móviles almacenan cantidades elevadas de información, tanto asociada a la configuración del sistema, como a las múltiples aplicaciones instaladas y a los diferentes servicios accesibles a través de los terminales, así como datos personales o corporativos de su propietario. Entre los datos almacenados se incluyen por ejemplo credenciales de acceso a servicios web e Internet, credenciales de cuentas de correo electrónico, mensajes de correo electrónico y telefonía (SMS/MMS), información de llamadas de telefonía, documentos privados y confidenciales, la agenda de contactos, el calendario con información de eventos y actividades, fotografías, vídeos, grabaciones de voz, listas de tareas, etc.

Una de las principales amenazas de seguridad en los dispositivos móviles actuales es el acceso a toda esta información mencionada por parte de un atacante, ya sea por disponer de acceso físico al dispositivo (de forma temporal o permanente), o por disponer de acceso remoto al terminal a través de una vulnerabilidad en alguno de sus componentes, o mediante una aplicación previamente instalada.

Por ejemplo SpyPhone fue en su día una aplicación desarrollada para el iPhone de Apple que permitía la obtención de información confidencial y personal almacenada en este tipo de dispositivos, incluso no habiendo sido aplicado el jailbreak .Los ejemplos de información obtenida por esta aplicación incluyen números de teléfono, lista de contactos, configuración de las cuentas de correo electrónico (salvo las contraseñas), las pulsaciones de teclado, búsquedas a través del navegador web, histórico de YouTube, las coordenadas recientes de localización a través del GPS, detalles de las conexiones a redes inalámbricas, capturas de pantalla, etc. Esta aplicación demostró en su día el riesgo asociado a la instalación de software aprobado por la tienda de distribución de

aplicaciones oficial del fabricante, dónde cualquier aplicación, haciendo uso de las librerías estándar, podía pasar los filtros de aprobación para su publicación y extraer información privada del usuario.

La información almacenada en el dispositivo puede ser protegida empleando mecanismos de cifrado, pero siempre debe tenerse en cuenta que el sistema operativo debe disponer de las capacidades necesarias para acceder a dicha información en tiempo real una vez se dispone de acceso al terminal. Es decir, pese al uso de cifrado en los soportes de almacenamiento, si un atacante consigue acceso al dispositivo, por ejemplo porque disponga del código de acceso o PIN, podrá acceder a los datos almacenados.

5.4 Localización

Los actuales dispositivos móviles, tales como los smartphones o las tabletas, disponen de capacidades de geo-localización (a través de sistemas GPS), lo que da lugar a la existencia de los llamados "servicios de localización". Estos servicios se han hecho muy populares y se usan con frecuencia en coordinación con otros, tales como: redes sociales, navegación, web browsers, etc.

Sin embargo, este hecho tiene implicaciones directas en la privacidad del usuario pues un atacante puede obtener información detallada de la ubicación en todo momento, lo que puede afectar gravemente a la privacidad del usuario, facilitando la creación de mapas geográficos de los movimientos de los usuarios y, en algunos casos, el tipo de actividad que desarrollan.

Las aplicaciones sociales basadas en la localización (Location-based social applications, LBSAs) suponen un riesgo para la privacidad de los usuarios, ya que se basan en la obtención de las coordenadas de la ubicación geográfica del usuario, para posteriormente procesarlas y ofrecer sus servicios.

En concreto, los dispositivos móviles actúan como clientes y envían su localización a servidores potencialmente no fiables. Los servidores disponen de la lógica de la aplicación para procesar la información de localización y ofrecer el servicio. Por tanto, los servidores recogen y almacenan cantidades elevadas de datos de localización de todos los usuarios.

Entre las medidas simples de seguridad que cabe adoptar en estos casos están:

1. Deshabilitar los servicios de localización de los dispositivos móviles.
2. Prohibir el uso de servicios de localización en relación con determinadas aplicaciones (redes sociales, fotografías, etc.)

5.5 Comunicaciones

Las amenazas de seguridad en dispositivos móviles emplean nuevos vectores de ataque a través de los mecanismos de comunicación empleados para la transferencia de información propios de estos dispositivos, como GSM (y el servicio SMS), GPRS, 3G y 4G o Bluetooth, así como vectores más tradicionales, como Wi-Fi, el acceso a Internet (TCP/IP) y la navegación web.

Las múltiples posibilidades de conexión de este tipo de dispositivos, tanto a redes privadas como públicas, permite la realización de ataques directos contra los mismos sin necesidad de tener que evitar controles de seguridad corporativos como cortafuegos perimetrales o sistemas de detección de intrusos.

Por otro lado las posibilidades de comunicación simultánea de los dispositivos a diferentes redes, como por ejemplo Internet y una red de datos privada, hace que los terminales actúen de pasarela entre diferentes infraestructuras, lo que facilita la realización de ataques y la propagación de malware entre entornos diferentes.

Es por ello que para las comunicaciones de datos a través de TCP/IP, tanto Wi-Fi como 2G/3G, se recomienda utilizar, siempre que sea posible, protocolos de comunicación seguros, es decir, autenticados extremo a extremo, y cifrados. Por ejemplo, acceder a sitios web mediante HTTPS en lugar de HTTP, configurar las aplicaciones de correo para que se conecten con el servidor mediante IMAPS en lugar de IMAP, emplear soluciones de mensajería instantánea que hagan uso de cifrado, y así sucesivamente con las diferentes alternativas de protocolos, cuando las haya. No obstante, es importante ser consciente de que en muchas ocasiones el usuario no puede elegir el protocolo o protocolos de comunicación que utilizarán las distintas aplicaciones.

A nivel corporativo es necesario definir una política de seguridad para los dispositivos móviles con capacidades NFC, Bluetooth y Wi-Fi, que analice su configuración por defecto y establezca la lista de dispositivos NFC y Bluetooth o redes WiFi permitidas, el tipo de información que estos pueden almacenar, y en qué tipo de entornos pueden ser utilizadas estas tecnologías, como por ejemplo dónde llevar a cabo el emparejamiento inicial entre dos dispositivos Bluetooth o si se permite la conexión a redes Wi-Fi abiertas. En ambos casos la concienciación de los usuarios finales acerca de las amenazas existentes juega un papel muy importante. Esta política debe ser monitorizada, por ejemplo, en los puntos principales de acceso a los edificios de la organización, permitiendo identificar dispositivos NFC, Bluetooth o WiFi no autorizados o mal configurados.

Las tecnologías inalámbricas (NFC, Bluetooth, WiFi, 2G/3G…) deben ser incorporadas a las auditorías de seguridad y pruebas de intrusión periódicamente planificadas sobre el resto de tecnologías empleadas por la organización, con el objetivo de identificar anomalías respecto a la política de seguridad definida así como debilidades y vulnerabilidades en los dispositivos móviles y en su utilización.

Finalmente, debe tenerse también en cuenta que las tecnologías inalámbricas son susceptibles de verse amenazadas de manera general por técnicas o ataques de

Denegación de Servicio (DoS), siendo trivial la generación de suficiente ruido en el espectro de radiofrecuencia asociado a una tecnología inalámbrica concreta (mediante dispositivos conocidos como jammers) para no permitir el uso de la misma.

5.5.1 Bluetooth

Las tecnologías inalámbricas Bluetooth (IEEE 802.15.1), estándar creado por Ericsson en 1994, permiten establecer comunicaciones de datos personales de corto y medio alcance entre dispositivos móviles, ordenadores personales y periféricos, reemplazando entre otros a los cables serie, paralelo o USB. Bluetooth es una tecnología de bajo consumo y bajo coste que no requiere disponer de una infraestructura o red de datos, pudiendo establecerse comunicaciones directamente entre dispositivos. Bluetooth permite comunicar múltiples dispositivos simultáneamente, a través de una picored, dónde un dispositivo actúa de gestor (o maestro) y es posible disponer de hasta 7 dispositivos adicionales (o esclavos). Un dispositivo Bluetooth puede incluso pertenecer a varias picoredes (scatternet).

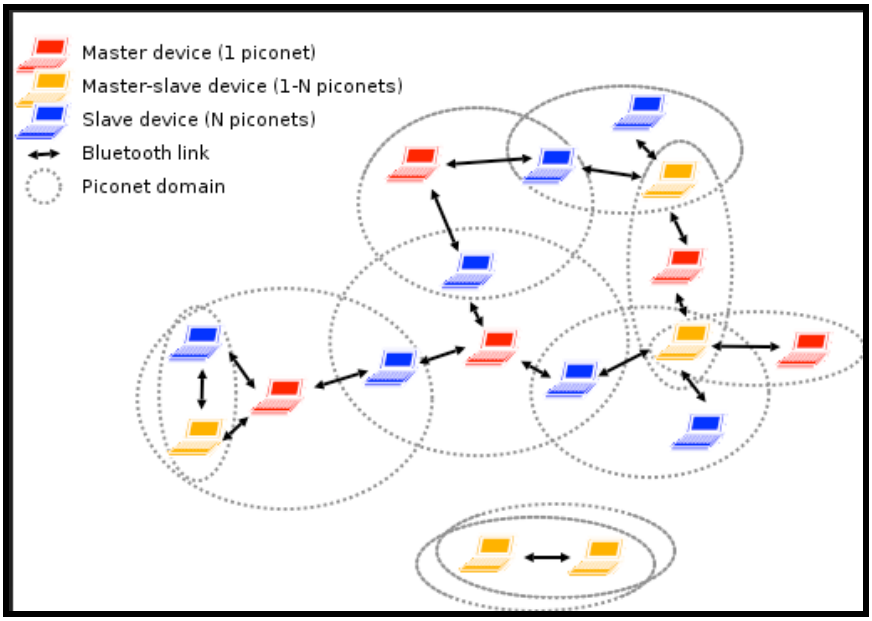


Figura 1. Ejemplo de comunicación por red Bluetooth

Bluetooth ofrece sus servicios a través de perfiles, cada uno de los cuales proporciona unas capacidades de comunicación específicas al dispositivo que lo implementa. Dentro de los perfiles más habituales existentes en los dispositivos móviles encontramos el perfil de emulación de puerto serie (RFCOMM), auricular o manos libres, altavoz, conectividad de datos (PAN, Personal Area Network), intercambio de ficheros y tarjetas de visita (OBEX FTP y Push), acceso a la SIM (SAP, SIM Access Profile), etc.

En la actualidad los fabricantes de dispositivos móviles han restringido notablemente los perfiles disponibles existentes en sus implementaciones, limitando así posibles vulnerabilidades de seguridad sobre los mismos.

El establecimiento de una comunicación Bluetooth tiene asociadas tres fases diferenciadas: descubrimiento (inquiry), en la que un dispositivo conoce la existencia de otro, conexión (paging), en la que se intenta establecer la comunicación con el otro dispositivo (incluyendo la primera vez el proceso de emparejamiento) y descubrimiento de servicios y capacidades (mediante el protocolo SDP, Service Discovery Protocol), para la identificación de los perfiles y funcionalidades existentes.

Desde el punto de vista de seguridad, Bluetooth implementa tres mecanismos de protección: autentificación, para verificar la identidad entre dispositivos - a través del proceso de emparejamiento en su primera conexión o a través de las claves de enlace en conexiones posteriores, autorización, para establecer el nivel de acceso y las restricciones sobre la utilización de los perfiles y servicios disponibles, y cifrado, para proteger los datos intercambiados con una clave derivada de la clave de enlace. Desde el punto de vista de la autorización es posible permitir acceso completo y no restringido a un perfil a cualquier dispositivo previamente emparejado (máxima confianza), acceso parcial a ciertos perfiles y con confirmación por parte del usuario, o ningún acceso. Desde el punto de vista del cifrado, es difícil determinar desde el punto de vista del usuario cuándo se hace uso del mismo - a nivel de la capa de enlace (LMP, Link Management Protocol), salvo en el caso de perfiles que no requieren de un emparejamiento previo, como OBEX Push, y que por tanto, no cifran las comunicaciones.

La tecnología Bluetooth ha sido objeto de múltiples análisis de seguridad y ataques en los últimos años, pero no por ello deja de seguir constituyendo un vector de ataque activo en los dispositivos móviles.

Un dispositivo con conectividad Bluetooth, en función de su configuración de seguridad, está expuesto entre otros a la captura de datos por parte de un tercero, afectando a la confidencialidad de las comunicaciones, ataques de diccionario o fuerza bruta sobre el PIN empleado durante la autentificación y ataques de suplantación de dispositivos previamente emparejados, afectando a la integridad, incluyendo ataques a través de conexiones o redes no fiables como las asociadas al marketing de proximidad, y ataques de denegación de servicio, afectando a su disponibilidad.

Concretamente, en el entorno de los dispositivos móviles, han existido numerosos especímenes de malware en el pasado que se propagaban mediante las capacidades de comunicación Bluetooth de los terminales, como Caribe (2004) o Comm Warrior.

Las características y funcionalidades añadidas en ocasiones por los fabricantes de los dispositivos móviles con el objetivo de mejorar las prestaciones del sistema operativo empleado pueden dar lugar a nuevas vulnerabilidades.

Las amenazas de seguridad de Bluetooth afectan principalmente a la privacidad del usuario, mediante la interceptación de las comunicaciones de voz y datos y el acceso a la información almacenada en los dispositivos móviles a través de Bluetooth. Técnicas como bluesnarfing permiten el acceso no autorizado a la lista de contactos, calendario, mensajes SMS, archivos, etc., del usuario a través del perfil OBEX Push. Adicionalmente, otra amenaza muy generalizada ha sido el fraude a través de Bluetooth mediante el uso no autorizado de los servicios de telefonía existentes en los dispositivos móviles, empleando técnicas como bluebugging, que permiten el acceso no autorizado a los comandos AT del terminal y la realización y redirección de llamadas y SMS a través del perfil RFCOMM. Por último, los ataques blueline permiten combinar técnicas de ingeniería social y aprovechar las limitaciones de tamaño de la pantalla de los dispositivos móviles para manipular el mensaje de autorización que se muestra al usuario antes de confirmar el establecimiento de una conexión Bluetooth.

Aunque teóricamente el rango de alcance de Bluetooth es de unos 100 metros, se ha demostrado la posibilidad de establecer conexiones de unos dos kilómetros mediante la utilización de antenas de alta ganancia, por lo que no debe asumirse que un potencial atacante únicamente estará en un rango cercano a la víctima.

5.5.2 NFC

Las tecnologías inalámbricas NFC (Near Field Communication), estándar creado a través del NFC Forum en el año 2004 por Nokia, Philips y Sony, permiten establecer comunicaciones de datos entre dos dispositivos próximos. La tecnología NFC emplea un rango de radiofrecuencia no licenciado, concretamente 13,56 Mhz. Estableciendo comunicaciones de corto alcance (10 cm teóricamente) con un ancho de banda de entre 106-424 Kbps. Los dispositivos NFC pueden operar en modo activo (empleando una fuente de energía) o pasivo (etiquetas o tags NFC).

NFC se emplea principalmente como sistema de pago por proximidad para la realización de pequeñas transacciones financieras, o micropagos, convirtiendo a los dispositivos móviles en medios de pago habituales. NFC permite el acceso a los datos de una tarjeta de crédito o débito almacenados en una tarjeta SIM (NFC) o en una billetera virtual (Secure Element) del dispositivo móvil, como por ejemplo a través del servicio móvil de pago Google Wallet, ampliamente utilizado en dispositivos móviles Android desde el año 2011 en USA. Por tanto, NFC habilita la realización de pagos en quioscos de autoservicio, aparcamientos, medios de transporte, etc. y tiendas sin disponer de tarjeta de débito o crédito, o de dinero en efectivo. Tras introducir el comerciante el importe de la transacción en el terminal punto de venta compatible NFC (como MasterCard PayPass, Visa payWave o American Express ExpressWPay), el pago se realiza cuando el usuario aproxima su dispositivo móvil a dicho terminal.

Adicionalmente, NFC puede ser empleado como mecanismo para simplificar el establecimiento de conexiones de datos a través de protocolos más complejos. Por ejemplo, Android Beam (disponible desde Android ICS), así como BlackBerry y Windows Phone 8, simplifican el intercambio de datos entre dispositivos (fotos, vídeos, contactos, direcciones, etc.) rápidamente a través de NFC, facilitando el establecimiento de una conexión Bluetooth, y realizando todo el proceso de activación y emparejamiento. De manera similar, los dispositivos móviles Samsung pueden establecer mediante NFC una conexión WiFi Direct para el intercambio de ficheros (S-Beam, Samsung-Beam).

Finalmente, los dispositivos móviles pueden hacer uso de etiquetas NFC para la automatización de tareas: cuando una etiqueta NFC específica es escaneada, el dispositivo puede ejecutar una o varias acciones previamente definidas y asociadas a dicha etiqueta, como por ejemplo cambiar la configuración del terminal, enviar un mensaje, realizar una llamada, o ejecutar una aplicación móvil concreta.

Figura 2. Ejemplo de comunicación NFC

Principales amenazas:

Debido a su reciente adopción y a las implicaciones económicas asociadas a NFC, esta tecnología constituye actualmente un área activa dentro de las investigaciones de seguridad. En julio de 2012 se demostraron públicamente en la conferencia BlackHat USA diferentes vulnerabilidades en la implementación NFC de dispositivos móviles Android (entre otros), como el Nexus S (Gingerbread) o el Google Galaxy Nexus (ICS), que permitían acceder a datos del usuario e incluso la descarga de código malicioso en los terminales, tras forzar al navegador web a visitar un sitio web concreto a través de esta tecnología sin la intervención del usuario. Por otro lado, durante el concurso Mobile Pwn2Own de la conferencia EuSecWest celebrada en Ámsterdam en septiembre de 2012, se demostraron vulnerabilidades en un Samsung Galaxy S3 con Android 4.0.4 (ICS) a través de NFC que permitían la ejecución de código en el dispositivo. Pese a que la vulnerabilidad fue explotada a través de NFC, también habría sido posible aprovecharla a través de otros vectores de ataque como e-mail o navegación web.

Pese a ser necesaria la proximidad entre dispositivos NFC para establecer una conexión, con el uso de antenas de alta ganancia es potencialmente posible capturar los datos intercambiados en un rango inferior a 10 metros (para conexiones activas) y 1 metro (para conexiones pasivas), frente a los 10 cm teóricos.

En la actualidad es posible llevar a cabo ataques de interceptación (o MitM) sobre NFC, conocidos como ataques de reenvío (o relay), donde un atacante en la ubicación adecuada puede interceptar, manipular y reenviar los datos intercambiados entre dos dispositivos NFC (activo y pasivo).

Medidas de protección:

Las opciones de configuración disponibles en la actualidad en los dispositivos móviles con soporte para NFC, como Android, son muy limitadas. Por este motivo, se recomienda deshabilitar el interfaz NFC

5.5.3 WIFI

Los dispositivos móviles están expuestos a la totalidad de las vulnerabilidades, amenazas y riesgos asociados a cualquier dispositivo informático con capacidades de comunicación a través de redes inalámbricas WiFi (IEEE 802.11).

Uno de los mayores riesgos de seguridad asociado a las comunicaciones de datos inalámbricas a través de redes WiFi es la conexión a redes públicas y abiertas, con un nivel de seguridad reducido o inexistente (sin mecanismos de autentificación y cifrado), no supervisadas por la organización propietaria del dispositivo, como por ejemplo hotspots WiFi disponibles en hoteles, aeropuertos o centros de conferencias.

Un dispositivo con conectividad WiFi, en función de los mecanismos de seguridad implantados en la red inalámbrica, está expuesto entre otros a la captura e interceptación de datos por parte de un tercero, afectando a la confidencialidad de las comunicaciones, ataques de inyección de tráfico y ataques de suplantación de la red,

afectando a la integridad, y a ataques de denegación de servicio, afectando a su disponibilidad.

Adicionalmente, una de las vulnerabilidades propias de los dispositivos móviles es la incorrecta integración por parte de los fabricantes de diferentes tecnologías de comunicación inalámbricas en un mismo dispositivo, desconociendo los requisitos de diseño de cada una de ellas.

La mayoría de dispositivos móviles actuales proporcionan conectividad mediante Bluetooth y WiFi. La asignación de las direcciones físicas (o direcciones MAC) para cada una de estas tecnologías se lleva a cabo de forma correlativa en muchos casos, es decir, el dispositivo móvil posee la dirección 00:01:02:0A:0B:0C en el interfaz Bluetooth, y la dirección (siguiente) 00:01:02:0A:0B:0D en el interfaz WiFi. Este hecho, propio del proceso de fabricación y registro de los dispositivos móviles, introduce una nueva vulnerabilidad inexistente al emplear las tecnologías de forma independiente. La dirección física del dispositivo en Bluetooth se emplea como un secreto, y es necesaria para establecer cualquier comunicación con él. Cuando el dispositivo es configurado en modo no visible, situación recomendable desde el punto de vista de seguridad, la dirección se oculta. Sin embargo, la dirección de un dispositivo en WiFi puede obtenerse de forma trivial mediante la captura del tráfico inalámbrico, ya que está disponible en las cabeceras de cualquier trama transmitida, situación que no puede ser evitada ni empleando los estándares WiFi de seguridad más avanzados, como WPA2 Enterprise. La práctica común de asignar direcciones correlativas expone por tanto la dirección Bluetooth del dispositivo una vez se conoce la dirección WiFi, introduciendo una nueva vulnerabilidad independiente de la tecnología o implementación de la pila de comunicaciones Bluetooth.

5.5.4 Comunicaciones móviles 2G/3G (VOZ, SMS y DATOS)

La telefonía móvil digital es un servicio que lleva con nosotros relativamente poco tiempo, y que ha evolucionado mucho en su corta andadura. La primera generación de telefonía móvil fue analógica. En España fue a partir de 1990, con el despliegue del servicio TMA-900, con el nombre comercial de Moviline, cuando comenzó a popularizarse la telefonía móvil.

Este servicio analógico no tenía ninguna ambición de protección de las comunicaciones: la información (voz, principalmente) viajaba en claro, simplemente modulada en frecuencia (FM), con lo que podía ser interceptada con un simple escáner de frecuencias. El servicio Moviline se mantuvo activo en España hasta diciembre de 2003, fecha en que se apagó definitivamente.

La segunda generación (2G) de comunicaciones móviles la constituyó el estándar GSM, desarrollado inicialmente por la CEPT (Conférence Européene des Administrations des Postes et Telécommunications) y posteriormente apoyado a nivel mundial por un gran número de empresas del sector. En España el servicio GSM comenzó a ofrecerse en 1995.

Este sistema, ya digital, sí que incluyó entre sus objetivos garantizar la seguridad y la privacidad de las comunicaciones. Por ello entre sus funcionalidades se contaba el

uso de criptografía tanto para la autenticación de los usuarios como para el cifrado de todas las comunicaciones.

El servicio GSM nació inicialmente sin la capacidad de transmitir datos mediante conmutación de paquetes. Sólo permitía establecer comunicaciones de datos punto a punto para, por ejemplo, transmitir un fax, y también enviar mensajes cortos (SMS). Posteriormente, no obstante, se ampliaría el servicio GSM, incorporándole los protocolos GPRS, primero, y EDGE después, que permitían (permiten) el acceso a Internet, aunque a velocidades bastante reducidas (236 Kbps en el mejor de los casos).

La tercera generación (3G) la constituye el estándar UMTS, desarrollado por el grupo de colaboración 3GPP (3rd Generation Partnership Project), compuesto por múltiples asociaciones de telecomunicaciones de todo el mundo. UMTS fue desarrollado como una evolución de GSM, de manera que la transición de GSM a UMTS fuese sencilla. En España se comenzó a ofrecer servicio UMTS en 2002.

UMTS nació desde el principio con la capacidad de conmutar tanto circuitos, para las llamadas de voz, como paquetes, para las conexiones de datos, como el acceso a Internet. Inicialmente la máxima velocidad de transferencia de datos era de 384 Kbps, pero posteriormente se añadieron los protocolos HSDPA, HSUPA y HSPA+, que aumentan la velocidad hasta un máximo teórico de 42 Mbps.

La cuarta generación (4G) la constituye el estándar LTE-Advanced, desarrollado también por 3GPP. Desde 2010 está siendo desplegado en diferentes partes del mundo. Este servicio es el primero que abandona la conmutación de circuitos, tradicional en el mundo de la telefonía, para basarse totalmente en conmutación de paquetes. Obviamente el envío de datos, aparte de las comunicaciones de voz, forma parte de este servicio desde su concepción, prometiendo velocidades de entre 250 Mbps y 1 Gbps.

La funcionalidad de SMS (Short Message Service) de los dispositivos móviles permite el envío de mensajes cortos empleando la infraestructura GSM (Global System for Mobile communications, o 2G) empleada para las comunicaciones de voz de la telefonía móvil (mediante conmutación de circuitos).

La especificación y la implementación del módulo SMS de los dispositivos móviles no soporta únicamente el intercambio de mensajes de texto, sino que también puede gestionar datos binarios, como tonos de llamada, y ficheros multimedia (audio, vídeo e imágenes), sobre todo en sus variantes avanzadas: EMS (Enhanced Messaging Service) y MMS (Multimedia Message Service).

5.6 Vulnerabilidades y amenazas multiplataforma

Uno de los riesgos inherentes a los dispositivos móviles es la propagación de malware desde los mismos hacia los ordenadores empleados para la compartición y transferencia de datos o sincronización. Es fundamental evaluar por tanto la posible propagación de software malicioso desde dispositivos móviles a otros entornos multiplataforma, como son equipos portátiles o de sobremesa.

Los dispositivos móviles actuales disponen de capacidades de almacenamiento interno o externo, mediante tarjetas tipo SD (Secure Digital), microSD, CF (Compact Flash), etc.

Cuando el dispositivo móvil es conectado a otro equipo para realizar la sincronización de los datos compartidos entre ambos o para transferir cualquier tipo de información, existe el riesgo de que malware residente en el dispositivo móvil sea transferido, y por tanto infecte el equipo al que se ha conectado.

Las conexiones se realizan habitualmente mediante cable USB, y el dispositivo móvil se ofrece como unidad de disco USB al equipo al que se conecta. Si dicho equipo no está configurado con las restricciones adecuadas de seguridad y, por ejemplo en entornos Windows, ejecutará automáticamente los contenidos de la unidad de disco (es decir, del dispositivo móvil) en el momento de su conexión, se podrá infectar.

Esta ejecución automática constituye un vector de ataque ya conocido para la propagación de software malicioso. Uno de los primeros especímenes de malware que empleaba esta técnica de propagación e infección entre dispositivos móviles Symbian y ordenadores Windows fue Cardtrap, descubierto a finales del año 2005.

La infección inicial del dispositivo móvil puede ocurrir a través del uso diario del terminal por parte del usuario, o directamente desde fábrica en dispositivos nuevos. Un ejemplo concreto de este último tipo de amenaza en entornos Windows fue descubierto en marzo de 2010 en dispositivos basados en Android y distribuidos por Vodafone en España. Vodafone distribuyó móviles HTC Magic en Europa con Android 1.5 que contenían en la tarjeta de memoria externa múltiples muestras de malware, concretamente, software cliente de la botnet Mariposa (una de las mayores botnets descubiertas hasta el año 2010 e investigada por la Guardia Civil), Confiker (uno de los gusanos de mayor distribución en entornos Windows en los últimos años) y Lineage (una herramienta de robo de contraseñas). La distribución de dicho espécimen de malware afectaba a todo aquel equipo Windows al que se conectara el dispositivo móvil mediante USB, y que tuviera activa la auto-ejecución (autorun) de unidades de disco. El malware no afectaba en este caso al propio dispositivo móvil, pero no existen limitaciones que hubieran evitado que así fuese.

El malware Mariposa, contenido en el fichero “AUTORUN.EXE”, se hospedaba en una carpeta denominada “NADFOLDER”, con fecha de creación el 1 de marzo de 2010.

Tras el incidente inicial, a los pocos días se confirmó otro caso similar en el mismo tipo de dispositivo, por lo que Vodafone realizó una investigación del incidente, confirmando la infección de un lote de 3.000 tarjetas de memoria microSD distribuidas con múltiples terminales de la operadora.

Este incidente enfatiza la necesidad de disponer de un proceso seguro en la fabricación, procesos de calidad y distribución de dispositivos móviles y sus diferentes componentes (como las tarjetas de memoria), desde su concepción en la fábrica hasta su entrega al usuario final.

La posibilidad de comprometer ordenadores tradicionales, como equipos portátiles o de sobremesa, a través de dispositivos móviles abre nuevas vías para penetrar el perímetro de seguridad de las organizaciones, que es vulnerado cuando el usuario conecta su terminal al ordenador ubicado en redes internas.

Notas tomadas de [CTRED]

Capítulo 6

¿Cómo prevenir? Mecanismos de Seguridad

En este apartado se abordarán todas las recomendaciones consejos y medidas de seguridad necesarias para prevenir, o minimizar el impacto de ser objeto de un fraude o un delito informático a través de la red.

6.1 Medidas de seguridad recomendadas

En este punto se recopilan los consejos y medidas de seguridad que recomiendan las principales autoridades del Estado con el fin de prevenir los ciberdelitos.

6.1.1 Consejos relacionados con su sistema

I. Sistema actualizado

- Es recomendable proceder de manera periódica a actualizar tanto el sistema operativo como el software instalado en el dispositivo. Se recomienda activar en el dispositivo la función de actualización automática, a día de hoy esta función suele estar disponible para la mayoría de los dispositivos.

- Se recomienda que se lleven a cabo copias de seguridad del sistema de forma periódica, así como la creación de puntos de restauración para así evitar la pérdida de información por algún tipo de incidente de seguridad.

II. Infecciones de malware.

- Se recomienda el uso de antivirus y firewall. En muchas ocasiones estas aplicaciones pueden descargarse de forma gratuita de la red y han demostrado ser para los sistemas informáticos un potente sistema de defensa y de protección.
- Si el sistema operativo es Windows, es también recomendable que se trabaje desde una cuenta de usuario que no disponga de privilegios de administrador, evitando así en muchas ocasiones la posibilidad e instalación de las citadas infecciones de malware.
- Se recomienda ser cautelosos en el uso de las redes P2P, pues está demostrado que estas son un una fuente importante de infecciones de malware. Para ello es aconsejable analizar las descargas llevadas a cabo desde este tipo de redes con el antivirus del que se disponga.
- Se aconseja no abrir correos electrónicos con procedencia desconocida, o correos no solicitados. Lo más recomendable es eliminar este tipo de correos sin previsualizarlos.
- Se debe utilizar siempre software legal. No se aconseja realizar descargas de software de la red, pues muchas fuentes de malware provienen por este tipo de acciones.
- Por último, se recomienda la instalación en el equipo informático de algún tipo de software anti-spyware, de forma que se puedan evitar y detectar a tiempo posibles intrusiones en el equipo mediante programas espías destinados a sustraer información del equipo del que se está haciendo uso.

6.1.2 Consejos relacionados con la navegación en Internet: Métodos y procedimientos a realizar para una mayor seguridad como usuario

I. Proteger la identidad

- Es recomendable utilizar contraseñas fuertes, es decir, que estén compuestas por más de 8 caracteres, y estén formadas por letras mayúsculas, letras minúsculas números y caracteres especiales.
- Si se reciben mensajes en los que se pida el reenvío del mismo a sus contactos, se recomienda no seguir esta cadena de mensajes pues este tipo de acciones suele tener un objetivo oculto por porte del emisor original como por ejemplo la recopilación de direcciones de correo electrónico para propósitos comerciales o algún tipo de engaño a los usuarios que reciban este tipo de información (hoax).

II. Estafas en la red

- Para evitar ser estafado en la red, se recomienda que se visiten páginas de confianza. Se debe hacer caso omiso a los vendedores que ofrecen súper ofertas. Se aconseja buscar en la red referencias de cualquier vendedor del

que estemos interesados en adquirir sus productos, antes de realizar cualquier tipo de compra. El usuario ha de ser precavido en las compras, especialmente con vendedores que digan residir en el extranjero y se aconseja el pago contra rembolso para evitar casos de compras en donde se envíe el dinero por adelantado y posteriormente no se reciba el artículo prometido a cambio. Los sistemas de envío de dinero por internet aportan al vendedor un alto grado de anonimato, de tal forma que será mucho más difícil la recuperación del mismo si se ha caído en una estafa.

- Se ha de prestar especial atención en el uso de programas de acceso remoto. Mediante estos programas y a través de internet es posible acceder a un ordenador, desde cualquier otro. Esta gran ventaja si se utiliza de forma ilícita supone un grave peligro en la seguridad del equipo informático.
- Otra pauta a tener en cuenta sobre las estafas en la red son los dominios. No es habitual que una empresa relativamente grande utilice en sus correos dominios como yahoo o hotmail, de recibir este tipo de correos se debe desconfiar, pues suelen poseer su propio dominio
- Herencias, concursos, premios que, casualmente, le han correspondido. No crea en ellos.

III. Riesgo en la banca electrónica

- Se recomienda acceder al sitio web de su banco introduciendo la dirección web directamente en la barra de direcciones del navegador, no se debe acceder a través de enlaces externos o mensajes de correo, pues puede que redirecciones al usuario a páginas web fraudulentas aparentemente originales.
- Se debe comprobar que tipo de comunicación se está empleando en la comunicación con su banco. Esta siempre se lleva a cabo a través de protocolos seguros (https).
- Se recomienda cerrar la sesión personal al finalizar sus consultas en su sitio web bancario, ya que si cierra la ventana del navegador sin haber cerrado previamente la sesión, existe la posibilidad de dejar una puerta abierta a través de la cual los delincuentes informáticos pueden acceder a su cuenta bancaria.

IV. Privacidad en redes sociales

- En las redes sociales, se recomienda a los usuarios limitar el acceso de la información que compartan a personas conocidas (amigos o personas de confianza). Cuanto más amplio sea el círculo de contactos (amigos de mis amigos y todos los usuarios), los riesgos a los que el usuario se ve expuesto son mayores, y por tanto existe mayor facilidad para que terceras personas dispongas de información privada
- Se aconseja no colgar fotografías ni vídeos privados que no le gustaría que se difundieran. Una vez en la red el derecho al olvido resulta complicado.
- Sea prudente a la hora de suscribirse a grupos o eventos. En muchos de ellos no se sabe con certeza a quién estamos permitiendo ver nuestros datos.
- Habilite la navegación segura (https) para dificultar el robo de contraseñas y escuchas en las comunicaciones.

6.2 Contraseñas seguras

A lo largo de toda nuestra vida como usuarios nos tendremos que registrar en múltiples plataformas a través de nombres y contraseñas que nos identifiquen como usuarios del mismo. La elección del nombre de usuario que escojamos es más trivial, no en cambio la de la contraseña, ya que en algunos casos el usuario será visible por todos, mientras que la contraseña nos permitirá autenticarnos.

Debido a la gran importancia en la elección de una buena contraseña, a continuación, daremos una serie de pasos a seguir para la elección de una segura y fácil de recordar, pero difícil de averiguar por otros.

Cuando queremos elaborar o intentar complicar un poco más las contraseñas para que sean más difíciles de adivinar, las basamos, incluso de modo inconsciente, en referencias o fechas simbólicas como nuestro cumpleaños, la matrícula del coche, el cumpleaños de nuestros hijos o nuestro aniversario de boda. Según un artículo de la página The Next Web la contraseña más utilizada en móviles es el 1234, una contraseña típica que facilita de manera considerable las opciones de acceder al móvil y saltarnos así la primera barrera de seguridad, así también el uso de nombres de mascotas o fechas de cumpleaños, se lo pone relativamente sencillo a los que quieran introducirse en nuestro sistema. También así se lo ponemos fácil a los hackers, pues simplemente con piratearnos el Facebook o entrar en alguna página web e investigarnos un poco, podrán ver alguno de estos datos y, a partir de ellos, buscar la combinación de entrada a nuestros servicios. Respecto a la elección del nombre de usuario, los hackers saben que casi todos los usuarios utilizan el mismo nick que tenemos en la dirección de correo electrónico. Conviene, por lo tanto, no caer en los tópicos ni en lo trivial e intentar ser mucho más inteligentes y blindar lo que ahora tenemos casi como un libro abierto.

Veremos ahora los 10 consejos básicos en los cuales nos podemos basar para la elección de una buena contraseña, obtenidos de una página web, y adaptados posteriormente:

1. Buscar siempre claves que tengan más de ocho caracteres. En función del número de caracteres que tenga una clave así serán las distintas combinaciones posibles, y por lo tanto más fácil será romperla para un hacker. Se consideran débiles las combinaciones menores de ocho caracteres, que pueden identificarse con programas generadores de combinaciones aleatorias, lo que se conoce como "la fuerza bruta".

2. Nunca usar solo números. Aunque pongamos claves de ocho o más dígitos, si usamos solo números, es cuestión de tiempo que un programa informático encuentre la contraseña y entre en nuestras páginas.

3. Tampoco usar solo letras ni palabras. Las letras se pueden combinar con robots hasta dar con la clave. Respecto a las palabras, siempre tienen una conexión simbólica con nuestro subconsciente, por lo que alguien que nos conozca un poco puede adivinar las claves si piensa en el nombre de nuestra pareja, nuestros hijos o nuestras mascotas.

4. Optar siempre por combinaciones alfanuméricas. Mezclar letras y números es la solución más segura porque se mezclan dos sistemas de clasificación, lo cual amplía mucho las combinaciones posibles. De todos modos, un hacker que tenga algunos datos personales sobre nosotros y mucha psicología puede adivinar las claves si no nos hemos esmerado en confeccionarlas. Debemos ser conscientes de que, de modo automático, siempre buscamos combinaciones fáciles de recordar y relacionadas con personas y

fechas importantes. Por lo tanto, lo mejor después de escribir la contraseña es revisar que no contenga señales personales.

5. Intercalar signos de teclado. Un truco que nos permitirá usar letras y números relacionados con nuestra vida sin peligro es intercalar símbolos como "#", "$", "&" o "%" aleatoriamente entre los caracteres de la contraseña. La presencia de estos caracteres es mucho más difícil de descubrir para hackers y robots.

6. Lo mejor son las claves aleatorias. Si podemos usar un programa generador de claves aleatorias, estaremos mucho mejor protegidos. La página Clave Segura ofrece de manera gratuita un generador de claves en el que se puede escoger tanto la longitud de la contraseña como la cantidad de caracteres alfanuméricos que usamos. Otros servicios como Passwordmeter miden el nivel de seguridad de las contraseñas que confeccionamos.

7. No utilizar la misma contraseña para todo. Parece una obviedad, pero es lo que hacemos la mayoría de los usuarios. Hay que tener una contraseña distinta para cada servicio. También es recomendable cambiar las contraseñas cada cierto tiempo. En la mayoría del mundo empresarial por ejemplo, el sistema te obliga a cambiar la contraseña cada 60 o 90 días.

8. Guardar las claves en un documento de texto. Como las claves seguras son muy difíciles, por no decir imposibles, de recordar, lo lógico es guardarlas escritas en un documento de texto, que utilizaremos para almacenar las contraseñas de todos nuestros servicios. Cada vez que debamos entrar a un servicio, tendremos que recurrir a este documento, que debemos proteger. Puede que sea pesado, pero es más seguro. La verdad que este documento supondría un arma muy valiosa si se nos olvidase en el ordenador y nos lo hackearan, por lo que la recomendación es que se encuentre siempre en una memoria flash extraíble, o escrito en algún documento físico.

9. Guardar el documento en un lugar seguro. Hay varias opciones para guardar el documento con nuestras claves. La primera es usar una memoria USB separada físicamente del ordenador y que solo enchufemos cuando queramos abrir el documento con nuestras claves. Debemos ser conscientes de que podemos tener el ordenador monitorizado por algún software malicioso -ocurre con mucha más frecuencia de la que creemos- o que alguien puede acceder a través de la conexión wifi si esta no es lo bastante segura. La segunda alternativa es guardar el documento en una copia de seguridad en un servidor de la red, con protocolos de cifrado de 128 bits o más. Podemos guardarlo en plataformas diseñadas para tales usos, como Clipperz. Bastará con abrir este servicio y acceder al documento. Eso sí: la contraseña de acceso a Clipperz tiene que ser altamente compleja, deberemos saber que si la perdemos también perderemos el resto de contraseñas.

10. Cerrar la sesión de los servicios a diario. Cuando apaguemos el ordenador por la noche o al salir de casa, la mejor opción es salir de todos los servicios de uso habitual, ya sean el correo electrónico, las distintas redes sociales donde participemos o las plataformas donde guardamos documentos para sincronizarlos, etc. Si alguien encendiera nuestro ordenador y no los hubiéramos cerrado, podría acceder fácilmente a tales servicios, ya que el navegador guarda las contraseñas si no le indicamos lo contrario. Por lo tanto, hay que indicar en el apartado de "Seguridad" de nuestro navegador que no recuerde ninguna contraseña. Al volver a usar el ordenador habrá que introducir todas las claves, pero evitaremos disgustos. En caso de que no cerremos todos los servicios cada vez que apaguemos el ordenador, lo más útil y eficaz sería proteger nuestra sesión de usuario en el ordenador, con una contraseña, lo más potente posible.

Encontramos un par de ejemplos perfectos de cómo crear una buena contraseña, en la guía sobre la seguridad de la Carlos III [UC3MSEG].

Ejemplo: Un buen sistema para elegir nuestra clave es utilizar frases que tengan sentido para nosotros y que estén formadas por grupos de letras y números. Un ejemplo sería:

Frase: "Yo, tengo 2 hermanas y 1 hermano"

Clave:Y,t2hy1h

Esta clave es fácil de recordar y sin embargo forma un conjunto de caracteres difícil de adivinar por un programa crackeador de claves.

O "Volverán Las Oscuras Golondrinas En Tu Balcón Sus Nidos A Colgar", daría VLOGETBSNAC. Ahora modificaríamos la contraseña para que tenga minúsculas, números y signos. Por ejemplo podemos sustituir las letras LO por los números 10, insertar una coma tras la G y pasar a minúsculas la V inicial, con ello la contraseña elegida sería v10G,ETBSNAC, fácil de recordar, pero difícil de adivinar.

6.3 Firma digital

El desarrollo de la era digital y con ello todas las medidas de comunicación telemáticas y de Internet ha facilitado el intercambio de mensajes de todo tipo, incluidos aquellos de contenido administrativo, entre distintas personas, organismos, países, etc.

Debido a esto es necesario, y cada vez más, la firma y autenticación de documentos, los cuales se vienen solventando con la firma digital o electrónica, ya que equivale, a todos los efectos, a la firma autógrafa, puesto que identifica fehacientemente la autoría del mensaje.

Físicamente hablando, la firma digital se constituye sobre la criptografía y puede ser expresada como una secuencia de bits (datos electrónicos) que se obtienen mediante la aplicación de un algoritmo (fórmula matemática) de cifrado asimétrico o de clave pública.

Estos sistemas se encargan de cifrar los mensajes mediante la utilización de dos claves distintas, una privada y otra pública. La clave privada es conocida únicamente por la persona a quien pertenece la firma o el par de claves. La pública, a su vez, puede ser conocida por cualquiera, para que se puedan descifrar los mensajes cifrados o firmados con la privada, pero no existe una relación matemática que nos permita obtener la clave privada a través de la pública.

La utilización de la firma digital asegura que ambos interlocutores, el emisor y el receptor del mensaje (ya sean dos empresarios, un empresario y un consumidor o un ciudadano y la Administración) puedan realizar una transacción fiable, garantizando la autenticidad de cada interlocutor. Para ello esos mensajes firmados electrónicamente tienen las siguientes características:

1.- Sirven para atribuir de forma irrefutable la identidad del signatario.

2.- Garantizan la integridad del mensaje, es decir, que el documento recibido sea exactamente igual al emitido, sin que haya sufrido ninguna modificación durante su transmisión.

3.- Aseguran el origen del mensaje de forma que el emisor no pueda repudiarlo o negar en ningún caso que el mensaje ha sido enviado por él mismo.

4.- Y por último, son confidenciales, es decir, el mensaje no ha podido ser leído por terceras personas.

Para obtener las claves pública y privada que se usan para firmar digitalmente estos mensajes es necesario dirigirse, bien personalmente o por medio de Internet, a una empresa o entidad que tenga el carácter de "Prestador de Servicios de Certificación" para solicitar el par de claves y su certificado digital correspondiente. El que se encargue de ser el prestador de servicios de certificación de firma electrónica deberá encargarse de comprobar la identidad del solicitante, bien directamente o por medio de entidades colaboradoras (Autoridades Locales de Registro), y entregará una tarjeta con una banda magnética en la que están grabados tanto el par de claves como el certificado digital. Con esa tarjeta magnética y un lector de bandas magnéticas adecuado conectado a un ordenador personal, se podrá utilizar la información de la tarjeta para firmar digitalmente los mensajes electrónicos.

En España existen varias autoridades certificadoras. La primera fue la Fábrica Nacional de Moneda y Timbre y luego se han ido sumando otras muchas, como ACE (Agencia de Certificación Electrónica), que está formada fundamentalmente por la banca, y ESTE (Fundación para el estudio de la Seguridad de las Telecomunicaciones), que está constituida por notarios, registradores, etc. Todas ellas emplean unos medios de identificación reconocidos jurídicamente y muy seguros.

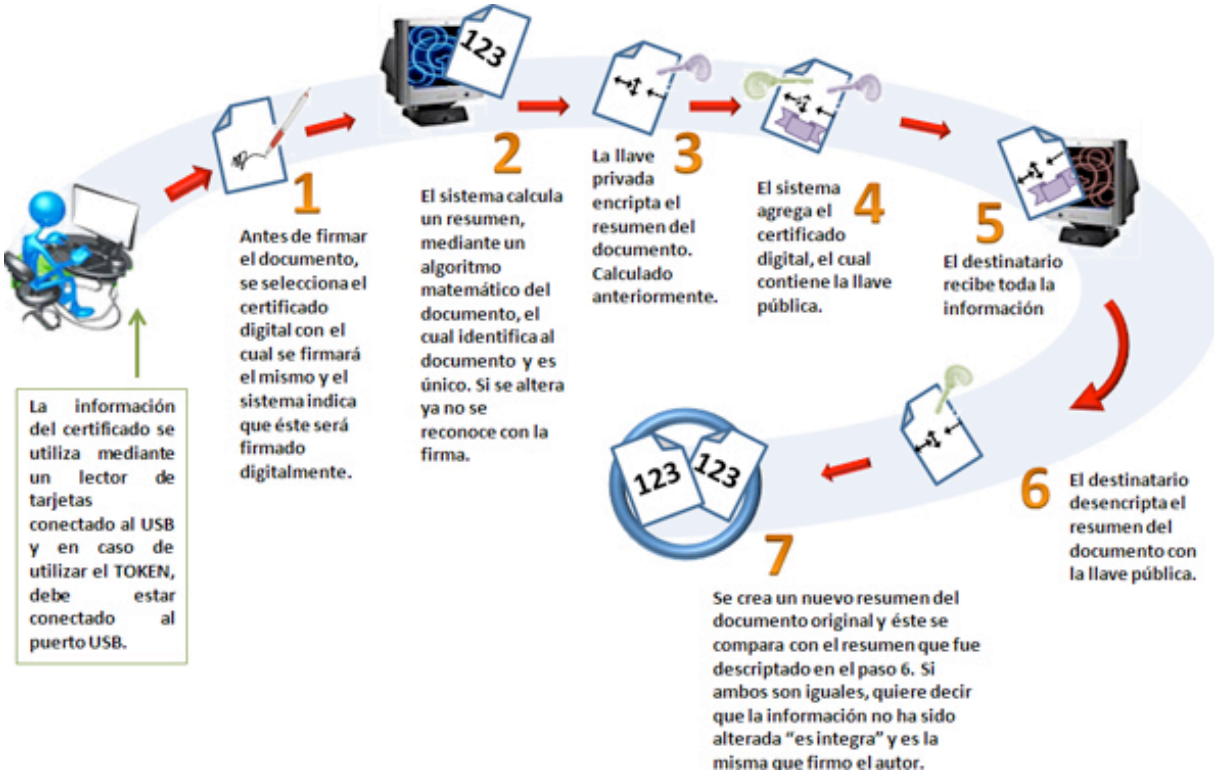


Figura 3. Firma digital

6.3.1 DNI Electrónico

La principal utilización de la firma digital en España es el DNI Electrónico, el cual aporta seguridad, rapidez, comodidad y la inmediata realización de trámites administrativos y comerciales a través de medios telemáticos. Hoy en día, está muy extendido el uso de los DNIs electrónicos, pues aportan una gran ventaja a la hora de realizar trámites en la administración pública para poder identificarse. Simplemente hace falta un pequeño lector de tarjetas conectado a un ordenador, para poder usarlo en cualquier emplazamiento. El DNI electrónico es una tarjeta de policarbonato que incorpora las más sofisticadas medidas de seguridad que harán virtualmente imposible su falsificación.

El Real Decreto 1553/2005, de 23 de Diciembre, por el que se regula la expedición del documento nacional de identidad y sus certificados de firma electrónica dice en su artículo 1.4: "Igualmente, el Documento Nacional de Identidad permite a los españoles mayores de edad y que gocen de plena capacidad de obrar la identificación electrónica de su titular, así como realizar la firma electrónica de documentos, en los términos previstos en la Ley 59/2003, de 19 de Diciembre, de firma electrónica."

6.4 Tarjetas de identificación

El propósito del sistema de tarjetas de identificación es controlar la entrada de una persona a un recinto determinado. Todo esto estará controlado por un sistema electrónico de apertura a través de la tarjeta.

Las tarjetas de identificación pueden ser utilizadas para distintas tareas, desde controlar la presencia de un individuo en una estancia determinada, llevar el control del tiempo que permanecen los empleados en la empresa o hasta llevar el control de accesos de personas a instalaciones. De todas maneras el sistema de control de presencia, se puede llevar a cabo a través de los otros, pues obviamente, si una persona ha entrado en un recinto y no ha salido, podemos concluir que sigue ahí.

El sistema de control de accesos aumenta considerablemente la seguridad de unas instalaciones, no sólo por el hecho de permitir la entrada al recinto o denegarla, sino también porque podemos restringir el acceso a determinadas áreas a algunos empleados.

Este sistema de control de accesos mediante las tarjetas de identificación ha ido evolucionando hasta llegar más recientemente al control por medio del chip de proximidad (radiofrecuencia, RFID). Este sistema de control de accesos mediante tarjetas plásticas permite, previa lectura del dispositivo, accionar la apertura de la puerta o torniquete quedando registrados en el sistema de seguridad los movimientos del portador de la tarjeta (entradas, salidas, movimientos internos en zonas restringidas, etc.). Lo que permite un completo conocimiento de qué ha hecho el usuario, a qué áreas ha entrado, etc....

Estas tarjetas sirven también para identificar a los usuarios pues son tarjetas que por lo general llevan la fotografía y datos particulares impresos, ya que la finalidad de las

tarjetas de control de presencia es mantener identificado en todo momento al portador de la misma.

No son exclusivas de los usuarios o trabajadores permanentes, también existen tarjetas para los visitantes en tránsito, a los cuales se les genera una tarjeta “in situ” ya que existen equipos de sobremesa que personalizan en un tiempo corto.

En general, su uso y aplicaciones están muy extendidos debido a las grandes ventajas que aporta, tales como:

- Sistema de identificación relativamente económico.

- Aumenta considerablemente la seguridad en las instalaciones.

- Conocimiento detallado y control de los datos de accesos de clientes, empleados y otras personas a las instalaciones (número de entradas, tiempos de permanencia...) ahorrando tiempo en la obtención de dichos datos.

Este tipo de tarjetas plásticas para el control del acceso están muy difundidas en: bibliotecas, universidades, hospitales, empresas, transporte, instalaciones deportivas, cadenas hoteleras, banca y por lo general en todas aquellas instalaciones que sean necesarias unas medidas de seguridad y un control de los accesos.

6.5 Escáneres biométricos

Estas tres medidas vistas anteriormente, permiten la identificación mediante algo que se sabe (una contraseña) o algo que se posee (la tarjeta de identificación), pero estas medidas de identificación cada vez son más sencillas de frustrar o de falsificar, pues las contraseñas se pueden adivinar y las tarjetas se pueden sustraer o replicar. Debido a todo esto surgió el desarrollo y posterior implantación de las medidas de control por sistemas biométricos, las cuales garantizan en gran medida, que la persona que accede al sistema es la que de verdad está acreditada para hacerlo.

Hoy en día cada vez hay más empresas y organizaciones que tienen como sistema de control de accesos los de reconocimiento biométrico debido a su gran tasa de eficacia y a su bajo nivel de falsificaciones. La siguiente información ha sido sacada de la bibliografía consultada del portal INCIBE.

6.5.1 Huella dactilar

Sin lugar a dudas, el más famoso y usado sistema biométrico de seguridad de los últimos años es la identificación basada en huellas dactilares. Esto es debido a que la mayoría de la población tiene huellas dactilares únicas e inalterables, incluso los gemelos o trillizos suelen tenerlas distintas (aunque rara vez se ha dado algún caso de gemelos con huellas iguales).

Es el rastro biométrico más utilizado, esto es así ya que tiene una alta tasa de precisión y que habitualmente los usuarios tienen conocimientos suficientes sobre su utilización. Aparte de esto, el pequeño tamaño de los receptores y su fácil integración a

los teclados o en las puertas, convierten a la huella dactilar en una tecnología muy útil y sencilla para su implantación y posterior uso en la seguridad de oficinas y hogares.

6.5.2 Reconocimiento facial

Otra técnica pero ya menos implantada, es la de reconocimiento facial, mediante la cual se reconoce a una persona a partir de una imagen o fotografía. Para lo cual, se utilizan determinados programas capaces de analizar las imágenes de rostros humanos. Entre otros parámetros estos programas se encargan de analizar la distancia entre los ojos, la longitud de la nariz o el ángulo de la mandíbula. Lo bueno de este sistema es que no solo se puede usar para el reconocimiento, sino también para la vigilancia en general mediante cámaras de video. El principal inconveniente de este sistema, es que hay que tener en cuenta que la cara envejece y cambia, al igual que es muy fácil alterarla poniéndose unas gafas o dejándose crecer la barba.

6.5.3 Reconocimiento de iris

También existe la posibilidad de identificar la identidad del individuo a través del iris humano. Los patrones del iris vienen marcados desde el nacimiento y rara vez cambian. El escaneado del iris se basa en una fotografía de alta resolución y en tan sólo unos segundos se puede verificar.

Cabe resaltar que este procedimiento es inocuo para el ojo, aparte de que se trata de una de las tecnologías biométricas más resistentes al fraude.

6.5.4 Reconocimiento de retina

Otro tipo de escáner ocular, es el de la retina, que se basa en analizar los patrones de los vasos sanguíneos contenidos en ella. El hecho de que cada patrón sea único (incluso para gemelos idénticos) y que se mantenga invariable a lo largo del tiempo, hace de este sistema el idóneo para entornos de alta seguridad.

6.5.5 Reconocimiento de la geometría de la mano

El último método, y la verdad el menos fiable, es el reconocimiento de la morfología de la mano. A través de determinados programas de análisis en 3D, se analizan la longitud y forma de los dedos, así como el tamaño de las articulaciones y demás características que definen la complexión de la mano. El inconveniente es que a cada cicatriz que se pueda producir, herida o inflamación, esta morfología puede variar, por lo que no resulta fiable al 100%.

6.6 Control de accesos

Como dijimos anteriormente, por norma general, suele existir un único sistema gestor central y por el contrario nos encontramos con una multitud de empleados con distintas jerarquías en las empresas los cuales, obviamente, no tendrán los mismos permisos de acceso al sistema.

De ahí, surge la necesidad de decidir entre los distintos permisos que debemos aplicar a las jerarquías. Por poner un ejemplo: en un entorno bancario, todos los empleados tienen acceso al sistema central para consultar el saldo de una cuenta, pero no desempeñarán las mismas funciones el personal de caja, que el director de la sucursal o que el jefe de área; cada uno tendrá un perfil de acceso distinto en función de las funcionalidades que su puesto requiera.

Este sistema de jerarquía debe permitir la herencia entre los perfiles, pues, volviendo al entorno bancario, un director de oficina podrá realizar exactamente las mismas operaciones que un cajero, aparte de las suyas propias, aunque un cajero no podrá desempeñar todas las funciones del director.

Uno de los mejores sistemas de gestión y control de accesos es el basado en roles, el cual veremos a continuación, aunque para verlo con mayor profundidad pueden consultar el portal de INCIBE.

6.6.1 Control de accesos basado en roles

La mejor alternativa para gestionar el control de accesos a gran escala es el sistema basado en roles o RBAC (Role Based Access Control).

Es una tecnología que ha tenido un gran auge ya que combina varias características principales de sus antecesores (listas de control de acceso, control de acceso discrecional y control de acceso obligatorio). Básicamente, el éxito de este tipo de control de accesos se basa en la forma jerárquica de funcionar que tienen los roles, ya que es más fácil administrar un sistema con roles asignados, y así poder llevar una administración de la seguridad más confiable y de menor coste.

La ventaja de este tipo de sistema es que es el propio administrador o propietario del sistema quien maneja los datos y asigna los roles, pudiéndose ajustar al máximo a las necesidades de la empresa.

Los permisos se encuentran asociados con los roles y los usuarios son miembros de esos roles. Los roles son creados en función de los distintos puestos que requiera la organización, y a los miembros se les podrá mover entre distintos roles, con lo que variarán sus permisos para adaptarse a las necesidades actuales de la entidad. Para ampliar la eficiencia de este sistema, nos encontramos con la herencia de roles, ya que un usuario podrá heredar los roles de otro usuario que esté a un nivel inferior.

6.7 Cortafuegos (FIREWALLS)

Los cortafuegos constituyen uno de los mecanismos de seguridad básicos en los entornos informáticos. Son programas que se integran en el sistema operativo o bien,

pueden ser instalados en los mismos y permiten controlar las conexiones que se producen entre dispositivos, ya sea vía Internet o a través de otro sistema.

Para los no muy versados en la materia, el intercambio de información entre clientes o servidores se produce a través de Internet y usando unos determinados protocolos y puertos. Los cortafuegos son como unos semáforos que dejarán establecer la conexión o no, por lo que se encargan de vigilar y controlar dichos puertos y conexiones para saber si permiten el flujo de datos o lo deniegan y así evitar envíos no deseados de información o conexiones entre clientes y servidores o a determinadas páginas que no queramos que se produzcan.

Podemos encontrar múltiples firewall distintos, además de que existen máquinas específicamente creadas para realizar las funciones de cortafuegos. Pero nosotros nos centraremos en dar algunas nociones sobre los de tipo personal, que son aquellos que, por regla general, ya vienen integrados en el sistema operativo.

El Firewall personal es el programa que se encuentra en la frontera entre nuestro sistema operativo y las aplicaciones de red, por lo tanto será el encargado de, tras comprobar una serie de parámetros, permitir o denegar el acceso. El sistema operativo si tiene instalado un firewall, le dejará a este por completo la elección de a qué programas se les permite el acceso y a cuales no.

Los cortafuegos de tipo entrante controlan los intentos de conexión que pretenden entrar en nuestro sistema, están pensados para controlar desde dónde se quiere acceder a un determinado servidor. Y los cortafuegos salientes son mucho más seguros, aunque por el contrario son los menos implantados y los menos usados. Su misión es controlar las conexiones que se realizan a otro servidor. Está pensado para comprobar a qué IP nos queremos conectar.

6.8 Medidas de seguridad físicas

Contra las amenazas naturales vistas anteriormente existen multitud de medidas que podemos tomar en consideración. En este apartado nombraremos algunas básicas que siempre debemos tener en cuenta.

Uno de los problemas más comunes que nos podemos encontrar en entornos tecnológicos son los problemas debidos a campos electromagnéticos y a posibles fallos de tensión. Todo equipo eléctrico produce un campo magnético que puede afectar a los equipos contiguos, ocasionando en algunos casos, pérdidas de datos relevantes. La mejor solución que podemos encontrar para minimizar al máximo este problema es el apantallamiento de los equipos a través de una malla metálica. En el caso de los fallos de tensión o pérdidas de la tensión pueden llegar a ocurrir que se pierdan los datos si nos falta la corriente durante un periodo considerable de tiempo. Una opción que encontramos cada vez en más empresas y administraciones públicas es la incorporación de un generador auxiliar o equipos compensadores que en caso de que falte la corriente o haya un fallo de tensión, el generador continuará con el suministro para que no se produzca ningún daño en los equipos o pérdida de datos.

Para solucionar posibles problemas de agua la mejor solución sería la impermeabilización, pero aun así para problemas de agua con mayor envergadura nos

encontramos con que eso puede que no sea suficiente, en cuyo caso lo mejor sería tener siempre una copia de seguridad, tanto de los ficheros físicos (que obviamente deberán estar en otro emplazamiento), como de los ficheros digitales que podrán estar copiados en otro lugar o subidos a alguna web. Aunque, para garantizar una buena evacuación del agua, será imprescindible contar con una buena ubicación y disponer de desagües y canales para poder evacuarla en caso de inundación o similar.

Algo parecido nos encontramos con el fuego o los terremotos. Para un fuego pequeño nos valdría con tener el fichero recubierto de algún material ignífugo que no emita gases tóxicos para que así no alimenten el fuego o disponer de almacenes aislados. En cambio, para fuegos de una magnitud considerable, lo recomendable sería, debido a la fuerza destructiva del fuego, poseer copias de seguridad en otro lugar, o si se trata de archivos físicos, digitalizarlos y subirlos a algún servidor web.

Para terremotos o seísmos de baja escala en los que no haya consecuencias físicas tampoco serían necesarias demasiadas medidas de seguridad, aunque si nos encontramos en zonas donde haya una gran presencia de temblores o posibilidad de que ocurran con una magnitud fuerte dentro de la escala de Mercallí o de Reigter, sí sería recomendable o desplazar nuestro emplazamiento, o en su defecto realizar copias de seguridad con cierta periodicidad y mandarlas a otro lugar, menos sensible a los movimientos sísmicos.

6.9 Antivirus

Los virus son programas informáticos cuya única finalidad es ejecutarse en un ordenador y corromper el resto de programas, ya sea destruyendo información, copiándola a otro ordenador, etc.

Debido al auge que experimentó este tipo de programas, surgieron los antivirus. Programas cuya función básica es detectar y eliminar los virus informáticos que se encuentren a su paso, así como todo tipo de programa malicioso.

Las funciones básicas que realiza un antivirus son: analizar los programas y archivos de nuestro ordenador y compararlos con una base de datos, donde se encuentran todos los códigos de los virus. De ahí, la importancia de tener nuestro antivirus actualizado, para disponer de la última versión de esa base de datos, no sea que en una comparación un virus relativamente nuevo no sea detectado.

Normalmente los antivirus cuentan también con componentes que se cargan en memoria y comprueban todos los archivos abiertos, creados o modificados en tiempo real, así como los archivos adjuntos de los correos electrónicos, scripts, etc.

Junto con los antivirus nos encontramos con los centinelas. Programas de pequeña envergadura que siempre acompañan a los antivirus, y que se encargan de controlar todos los ficheros con los que trabajas en tu ordenador, alertándote en caso de encontrar algo que ponga en riesgo la seguridad de tu equipo.

Softonic realizó un estudio donde analizaron los antivirus comerciales y elaboraron un ranking con los 5 mejores del mercado del 2015. El ranking donde se tienen en cuenta los resultados de protección y de rendimiento queda de la siguiente manera:

1.- Bitdefender. Es el número 1 del ranking debido al rendimiento, el usuario de hoy en día no quiere sacrificar velocidad por una seguridad no siempre eficaz.

2.- Kaspersky. Se caracteriza por sus 4 escudos en tiempo real, su Widget en el Escritorio y por una inmejorable tasa de detección.

3.- Avira. Su característica principal es que consume muy pocos recursos.

4.- Norton. Siempre ha destacado por su alta eficacia, pero ha bajado puestos debido a que consume bastantes recursos.

Se puede encontrar el ranking en el siguiente enlace (http://articulos.softonic.com/comparativa-antivirus-gratis-pago?ex=SWH-1566.0).

6.10 Monitorización de ordenadores

Normalmente las funciones de monitorización de ordenadores son llevadas a cabo por agentes (programas) que se encargan del seguimiento y registro de la actividad.

Como nunca sabemos si el peligro viene desde fuera de la empresa o dentro (pueden darse casos de empleados desleales), la organización puede elegir qué actividades monitorizar. Éstas pueden ser:

- Ejecución de copias de archivos.
- Entradas y salidas de usuarios en la red.
- Arranque de determinadas aplicaciones o programas.
- Registro de cambios relevantes producidos.

En función de la necesidad o la frecuencia con que ocurran los hechos, podremos programar que se nos avise de una forma u otra, ya sea mediante mensajes al móvil, envíos de correos electrónicos o que se almacenen estos avisos en un archivo para su posterior revisión

6.11 Acceso a terceros desde ordenadores externos (Token RSA)

Debido a la gran expansión que sufren algunas organizaciones cada vez se hace más necesario el uso de la intranet de la empresa o administración desde cualquier ordenador externo a la red, con el inconveniente de que las medidas de seguridad se verán mermadas al acceder desde un ordenador personal o desde cualquier otro terminal que no sea uno de la misma entidad.

Para lograr un acceso eficaz y fiable los usuarios tendrán que identificarse con dos factores exclusivos, algo que saben y algo que conocen, antes de permitirles el acceso.

Este tipo de tarjetas inteligentes fueron desarrolladas y explotadas por RSA Security que las incluyeron con la clave simétrica y su pin protegido. Además les aportaron las credenciales correspondientes y las hicieron soportar un registro único con RSA.

Este tipo de sistema de autenticación ofrece una alta seguridad frente a otros sistemas ya que tienen una clave simétrica que se combina con el algoritmo para generar el código de un solo rol cada 60 segundos. Que el código varíe cada 60 seg. hace de este sistema algo extraordinario, pues sería muy difícil que alguien que quiera acceder al sistema de forma ilícita, averigüe la clave en menos del minuto que dura, antes de que cambie.

Otra de las grandes ventajas de estos dispositivos es que debido a su utilidad pueden ser utilizados por empleados, personal asociado a la entidad, comerciales y clientes, los cuales las pueden llevar siempre encima debido a su pequeño tamaño y acceder siempre así al sistema.

6.12 Borrado seguro

Recordemos que las empresas son las encargadas de gestionar todos nuestros datos, no sólo en el momento en que sean recopilados y utilizados, también se deben encargar, a la hora de ser destruidos, de velar porque se haga de forma adecuada.

Aunque la verdad que esta destrucción de la información nunca suele llevarse a cabo de manera eficaz, pues siempre puede quedar algún tipo de residuo de información recuperable que vulnere la ley de Protección de Datos de Carácter Personal. De manera que veremos algunos tipos de borrado, en función del tipo de soporte que tengamos para la información, que garanticen un correcto borrado evitando así que los datos sean recuperados.

6.12.1 Desmagnetización

Este tipo de borrado sólo se puede aplicar a dispositivos magnéticos, tales como disquetes o cintas magnéticas. Se basa en la exposición de los dispositivos a un campo magnético que borre todos los datos contenidos en el dispositivo.

El tipo de campo magnético al que tengamos que exponer el dispositivo variará en función del soporte que se pretenda borrar, así como de su tamaño y forma, para así asegurar una correcta polarización de todas las partículas, y un correcto borrado.

Tras un proceso de esta envergadura hay determinados dispositivos que pueden no funcionar correctamente, lo que ocasiona un inconveniente, y es que dificulta la posterior comprobación de que todos los datos hayan sido borrados. Otra contraindicación es que por norma general, se suele optar por aplicar la potencia más alta del campo magnético en vez de estudiar la intensidad adecuada, lo que supone un desperdicio de energía.

6.12.2 Destrucción física

El objetivo de este proceso es la completa destrucción del medio de almacenamiento. Nos podemos encontrar con diferentes métodos que garanticen esta correcta inutilización del soporte, tales como:

o Fusión e incineración: Se suelen llevar a cabo en fundiciones o en plantas de incineración, y destruyen por completo el medio físico de almacenamiento.

o Trituración: Se suele usar cuando el medio físico donde se encuentra la información es el papel. La trituración se lleva a cabo por máquinas trituradoras especiales. El tamaño de la información de los residuos será directamente proporcional a la confidencialidad de los datos, cuanto más sensibles sean los datos más pequeños serán los pedazos. Los soportes de tipo óptico, como los CD o DVD, deben destruirse mediante pulverización o incineración, en destructoras determinadas.

Para la destrucción física es necesario algún tipo de certificación que garantice que la operación de destrucción se ha llevado a cabo correctamente, y no es posible acceder a la información eliminada. Este tipo de destrucción obliga en la mayor parte de las ocasiones, al transporte de los dispositivos hasta el centro de destrucción extremando además las medidas de custodia durante el traslado, lo que aumenta el coste.

6.12.3 Sobre-escritura

Normalmente, con el borrado lógico no se borran los registros, sino que lo que se suele hacer es poner el indicador de registro a cero, aunque la información se suele seguir conservando, esto permite un posible acceso futuro a la información que ya creíamos borrada. Para evitar esta situación, utilizamos el método de sobre-escritura, basado en escribir un patrón de datos (todo ceros, o ceros y unos o algo similar) sobre los datos que queramos eliminar.

Este método es tremendamente útil para aquellos dispositivos regrabables, pero ineficaz en los no regrabables como los CD y DVD, para los cuales tendremos que usar otro método de eliminación de la información como la destrucción de los propios soportes. Además, otras ventajas con las que contamos es que este proceso se puede desarrollar dentro de las empresas, eliminando el coste del transporte, y se puede verificar también la efectividad del borrado accediendo al dispositivo.

Capítulo 7

Organismos. Implantación de la Seguridad de los Dispositivos Móviles.

La implantación de las medidas de seguridad para dispositivos móviles en un determinado organismo debe desarrollarse en torno a una estrategia previamente definida, que ayude a las organizaciones a determinar cuando el despliegue de una determinada medida de seguridad puede ser importante para preservar los activos de información o los servicios del organismo.

En los siguientes párrafos desarrollaremos la estrategia recomendada por el ENS (Esquema Nacional de Seguridad), que a pesar de que solamente obliga a las entidades publicas es un buen marco a tener en cuenta por cualquier tipo de entidad. Esta estrategia está basada en la utilización de un modelo tradicional de implantación en cinco fases

Las fases consideradas son las siguientes:

- Iniciación
- Desarrollo
- Operación y Mantenimiento
- Retirada

Seguidamente se desarrollaran los aspectos esenciales de cada una de las fases enunciadas.

7.1 Iniciación

Esta fase comprende distintas acciones preparatorias entre las que cabe destacar:

- Identificar las necesidades presentes y futuras del organismo, en relación con el uso de dispositivos móviles.
- Especificar los requisitos funcionales y de seguridad que se prevén.
- Desarrollo de la Normativa de Seguridad en el Uso de Dispositivos Móviles, conteniendo:
  - ✓ Determinación de los recursos del organismo que podrán ser accedidos a través de dispositivos móviles.
  - ✓ Tipos de dispositivos móviles permitidos para acceder a tales recursos.
  - ✓ Nivel de acceso que poseerán por defecto las diferentes clases de dispositivos móviles (por ejemplo, los dispositivos móviles propiedad de los usuarios frente a los dispositivos móviles de titularidad del organismo).
  - ✓ Modelo de distribución de los equipos.
  - ✓ Modelo de gestión y administración centralizada de los dispositivos móviles.
  - ✓ Mecanismos de actualización de políticas y tecnologías de seguridad aplicables.

Es muy importante que la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo esté documentada y permanentemente actualizada, formando parte coherente del conjunto de normas de seguridad que desarrollan la Política General de Seguridad de los Sistemas de Información del organismo.

Cuestiones específicas relativas al modelo BYOD

En caso de que se plantee en el organismo la utilización del modelo BYOD, su implantación puede realizarse bajo tres perspectivas:

- Virtualización: Proporcionando acceso remoto a los sistemas de información corporativos, por lo que no habrá datos o ejecución de aplicaciones en el dispositivo personal.
- Aislamiento: Haciendo que los datos o las aplicaciones corporativas se encuentren dentro de un contenedor seguro (sandbox), aislado de los datos y aplicaciones personales de su propietario.
- Coexistencia controlada: Permitiendo en el dispositivo la convivencia de datos y aplicaciones corporativas con datos personales, contemplando las políticas de seguridad adecuadas que garanticen que los controles de seguridad se mantienen en todo momento.

Las especiales circunstancias, y los importantes riesgos, que rodean el uso de dispositivos móviles cuando el organismo ha aceptado el modelo BYOD para el desempeño de sus funciones, requiere tener en cuenta las siguientes cuestiones adicionales:

1. Normativa de Seguridad BYOD: Antes de investigar sobre la idoneidad o no de adoptar una determinada solución MDM, es necesario redactar, aprobar, solicitar y obtener de los propietarios de los dispositivos móviles el consentimiento informado en relación con la Normativa de Seguridad BYOD del organismo (incluida en la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo) y, en su caso, las Normas y Procedimientos de Seguridad derivados.

2. Seguridad Jurídica: Tal vez el mayor riesgo de BYOD es el peligro de revelación de información confidencial si el dispositivo se pierde o es robado. Por este motivo, la mayoría de las Políticas de Seguridad requieren el uso de contraseñas para el acceso, el bloqueo del dispositivo o el cifrado de información, así como el derecho institucional a borrar remotamente los datos del dispositivo, cuando se dan ciertas condiciones, incluyendo la finalización de la relación de trabajo del empleado púbico (o del colaborador, proveedor, subcontratista, etc.). Como se ha explicado, ciertas tecnologías permiten aislar los datos y aplicaciones corporativas del resto de contenidos del dispositivo, lo que posibilita eliminar de forma selectiva sólo lo que es necesario para el mantenimiento de las condiciones de seguridad institucionales. Si no se utilizan tales tecnologías, se eliminarían todos los datos del dispositivo móvil, incluyendo datos e informaciones personales del usuario, lo que podría provocar litigios, si no existiera una política de seguridad previa y claramente definida y formalmente aceptada.

3. Responsabilidades de los usuarios: Los usuarios tienen que entender sus responsabilidades, entre ellas el mantenimiento permanente de las medidas de seguridad hardware y software exigibles en cada caso (por ejemplo, mantener los parches de seguridad permanentemente actualizados). La Normativa de Seguridad BYOD del Organismo podría advertir de la desactivación automática de aquellos dispositivos que no cumplan tales medidas.

4. Actividades permitidas: La Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo determinará lo que está permitido y lo que no lo está, en relación con el uso de dispositivos móviles. Las limitaciones más frecuentes contendrán normas contra la descarga de datos o documentos corporativos, el acceso a determinadas redes o aplicaciones, o el uso de determinadas características del dispositivo, tales como cámaras o puertos USB, la prohibición del jailbreak o rooteado del dispositivo, y la determinación de listas blancas y listas negras de aplicaciones y sitios web. Algunas herramientas MDM alertan a los usuarios de posibles no conformidades con la política de seguridad y son capaces de bloquear el acceso hasta que se tomen medidas adecuadas.

5. Dispositivos permitidos: En determinados casos, puede ser conveniente que la Normativa de Seguridad BYOD limite los dispositivos móviles permitidos por el organismo, en aras a la reducción de gastos de soporte y a la eficiencia en la aplicación de controles de seguridad.

6. Servicios de soporte (Help/Desk): La decisión más rigurosa pasaría por hacer responsables a los usuarios cuando el dispositivo no funcione adecuadamente. Sin embargo, esto podría ir contra el principio de productividad en el que se asienta BYOD. Por tanto, será necesario encontrar soluciones de compromiso en las que el organismo asuma el soporte respecto del uso institucional del dispositivo, dejando al usuario la gestión de la problemática particular. Esta solución, matizable en niveles, puede

complementarse con la creación de foros de discusión y ayuda a los usuarios en las intranets corporativas.

7. Asunción de costes: Cuando el organismo en cuestión acepta el modelo BYOD, surge la pregunta de quién corre con los costes, tanto del propio dispositivo como los cargos por su uso. Parece lógico pensar que si la mayoría del tráfico de datos está relacionado con la actividad profesional, los usuarios confiarán que sea el organismo quién asuma los gastos corrientes. No obstante, para evitar situaciones no deseables, los organismos podrán establecer límites. En cualquier caso, los detalles del pago deberán explicitarse en la Normativa de Seguridad BYOD del organismo.

Criterios para adoptar (o no) el modelo BYOD

Se suele afirmar que permitir que los empleados públicos (y, en su caso, colaboradores, proveedores y subcontratistas) usen sus propios smartphones y tablets podría incrementar la satisfacción de los usuarios, mejorar la productividad y rebajar los costes del organismo, pero este modelo también tiene posibles inconvenientes. Seguidamente se incluyen diez cuestiones que conviene analizar con cuidado para determinar si el modelo BYOD es adecuado o no para una determinada organización.

1. Resistencia de los usuarios a asumir costes: Por regla general, los usuarios se resisten a correr con los gastos corrientes de sus propios smartphones o tablets cuando se usan para propósitos profesionales. La resistencia al pago se extiende tanto a la adquisición del dispositivo como a los posibles gastos mensuales relativos a su uso en redes de telecomunicaciones públicas o a los gastos de mantenimiento, reparación, etc. Esta circunstancia exigiría al organismo disponer de políticas de compensaciones que, en muchos casos, no será fácil acometer.

2. Problemática reducción de costes: Muchos Responsables de Sistemas están entendiendo que la adopción del modelo BYOD puede introducir a la organización en una espiral de costes. Sostienen esta afirmación alegando que: 1. Las organizaciones pierden la capacidad de reducir costes mediante la compra masiva de dispositivos móviles y 2. Pueden terminar pagando más de lo debido si se asumen determinados costes como reembolsables.

3. Complejidad añadida para el Departamento de Sistemas de Información: Permitir que los usuarios utilicen sus propios equipos añade complejidad a la gestión de los Departamentos de Sistemas de los organismos. Aunque la Normativa de Seguridad BYOD del organismo que se trate asigne a los usuarios la responsabilidad del soporte a sus propios equipos, esta situación puede no ser más que un espejismo, toda vez que los Help-Desk corporativos seguirán constituyendo el primer punto de contacto cuando algo no funcione adecuadamente. Además, la necesidad de adoptar nuevas medidas de seguridad para hacer frente al incremento de dispositivos móviles personales constituye un coste nada despreciable en el corto plazo. A este coste hay que añadir el derivado de la adquisición del nuevo software que será preciso implantar, tal como el requerido para: la protección de datos en los dispositivos móviles, el control de acceso a la red y la propia gestión de dispositivos móviles (soluciones del tipo MDM y/o MAM), y su instalación, implantación y mantenimiento.

4. Discriminación profesional: Permitir el modelo BYOD puede crear, involuntariamente, un entorno de trabajo desigual. Si el personal tiene que incrementar su gasto para mantenerse al día con respecto a sus compañeros, esta situación puede afectar negativamente a la moral y, por ende, a la productividad. (Si, por ejemplo, un empleado

público invirtiera una importante cantidad de dinero en adquirir un dispositivo de gama alta con el que pudiera desarrollar su trabajo más rápidamente, es más que probable que esta circunstancia conduzca a una situación incómoda con su propio entorno. Por el contrario, el uso de dispositivos propiedad del organismo evita el problema. Se trata del paradigma clásico del "uniforme escolar")

5. La asunción de responsabilidades: Como se ha dicho antes, la seguridad es uno de los mayores problemas con el que debe enfrentarse el modelo BYOD toda vez que permitir el uso de dispositivos de titularidad privada en las redes corporativas conlleva riesgos significativos, si tal despliegue no se gestiona correctamente. Estos riesgos son tan elevados que su uso suele estar terminantemente prohibido cuando se trata de posibilitar el acceso o tratamiento de información sensible, tanto de naturaleza personal como comercial. Puesto que los Departamentos de Sistemas de los organismos tendrán sobre los dispositivos BYOD menos control que si se tratara de dispositivos proporcionados por la propia organización, gran parte de la responsabilidad de la adopción de las medidas de seguridad recaerá en los propios usuarios. Para el usuario individual esto puede suponer un grave inconveniente, que será visto como una carga profesional añadida.

6. Pérdida de datos: De manera análoga a lo que sucede con los sistemas de información corporativos, también existe el riesgo de que se destruyan datos sensibles que previamente se han cargado en los dispositivos móviles propiedad de los usuarios.

Aunque las modernas soluciones MDM-MAM pueden reducir este riesgo, los usuarios pueden ser reacios a permitir el acceso a sus dispositivos de tal tipo de software. Como hemos visto, el Responsable de Seguridad y el Responsable del Sistema tienen la responsabilidad de la protección de los datos corporativos (haciendo una limpieza remota cuando alguien cesa en sus funciones), sin correr el riesgo de poner en peligro los datos personales del individuo.

7. Novedad vs. eficacia: Una de las características más atractivas de BYOD es la posibilidad que tiene el usuario de utilizar dentro de la organización la tecnología más novedosa (o más espectacular) en cada momento, ventaja que es aún mayor si la política BYOD corporativa comporta subvenciones económicas para la compra de dispositivos. No obstante, pasados los primeros momentos de euforia, la realidad del día a día puede ser diferente, sobre todo si los equipos no funcionan como era de esperar y los usuarios han de asumir las consecuencias de una inapropiada elección.

8. El problema de las licencias: El modelo BYOD exige mantener una permanente vigilancia sobre las licencias del software que se instale en cada uno de los dispositivos, lo que puede acarrear importantes costes. Además, atendiendo a las condiciones impuestas en determinadas licencias, el software en cuestión sólo podrá instalarse en dispositivos propiedad del organismo, lo que constituye una complicación añadida. Pueden presentarse, asimismo, otras cuestiones de naturaleza jurídica que es necesario contemplar y tratar adecuadamente

9. La productividad, en tela de juicio: Conviene valorar el riesgo que existe para la productividad si se anima a los empleados públicos a utilizar sus propios dispositivos, en general, más adecuados para el ocio (visionado de videos, juegos, acceso a redes sociales, etc.) que para el trabajo.

10. No todo el mundo es un apasionado de la tecnología: Se tiende a olvidar que no todas las personas (todos los usuarios, en nuestro caso) son apasionadas de la tecnología. Estos usuarios no se mostrarán nunca especialmente proclives al BYOD.

Limitaciones al uso de dispositivos móviles en función de los niveles de acceso

Como regla general, la Normativa de Seguridad en el Uso de Dispositivos Móviles del organismo, atendiendo a razones de seguridad, limitará los tipos de dispositivos que pueden ser usados para acceder a los recursos del organismo.

Tales limitaciones pueden establecerse en base a Niveles de Acceso, de la forma:

Nivel de Acceso Máximo	Posible Política: Solo los dispositivos móviles proporcionados y gestionados por el organismo podrán tener acceso a los recursos corporativos
Nivel de Acceso Intermedio	Los dispositivos móviles propiedad de los usuarios (BYOD) que se encuentren comprendidos dentro del ámbito de gestión centralizada de dispositivos móviles del organismo (y que, en su consecuencia estén ejecutando el software cliente correspondiente), podrán acceder a un conjunto predefinido de recursos corporativos
Nivel de Acceso Mínimo	Posible Política: Los dispositivos móviles propiedad de los usuarios (BYOD) que no se encuentren comprendidos dentro del ámbito de gestión centralizada de dispositivos móviles del organismo sólo podrán acceder a unos pocos recursos corporativos, tales como el correo electrónico, por ejemplo; o no podrán usarse en el organismo

Tabla 2. Niveles de acceso de los organismos desarrollados para limitar el riesgo.

Esta estratificación en niveles permite a los organismos limitar el riesgo, toda vez que los dispositivos no gestionados por la organización dispondrán únicamente de los privilegios mínimos.

Los Niveles de Acceso que cada organismo decida adoptar vendrán determinados por el correspondiente análisis de riesgos. En tal sentido, y a título de ejemplo, el cuadro siguiente enumera aquellos factores que los organismos podrían considerar a la hora de desarrollar su Normativa de Seguridad en el Uso de Dispositivos Móviles.

SENSIBILIDAD DE LA INFORMACIÓN MANEJADA	En ocasiones, determinadas actividades comportan el acceso a información sensible. En su consecuencia, deberán elevarse los requisitos de seguridad exigidos para el tratamiento de este tipo de información. Un ejemplo de ello sería la exigencia de que los usuarios solamente pudieran usar dispositivos suministrados por el organismo y/o limitar su uso remoto fuera del perímetro de seguridad de la organización.
CUMPLIMIENTO DE LA NORMATIVA DE SEGURIDAD EN EL USO DE DISPOSITIVOS MÓVILES	La mayor parte de los requisitos de seguridad del organismo sólo podrán alcanzarse cuando la organización tenga acceso a los controles de configuración de cada uno de los dispositivos. Por tanto, cuando un dispositivo no se encuentre dentro del ámbito de gestión centralizada de

	seguridad, será necesario que el servidor de la organización desarrolle algunas acciones preventivas cuando tal dispositivo pretenda acceder a recursos corporativos. Para evitar esta problemática, los organismos pueden decidir incorporar a su normativa de seguridad en el uso De dispositivos móviles la exigencia de que todos los dispositivos móviles ejecuten el software-cliente de gestión de seguridad proporcionado por la organización.
COSTE	Obviamente, los costes asociados al mantenimiento de la seguridad de los dispositivos móviles dependerán de las decisiones adoptadas en la normativa de seguridad en el uso de dispositivos móviles del organismo, distinguiendo entre costes directos (los correspondientes a cada uno de los dispositivos y al software-cliente instalado en ellos) y costes indirectos (los derivados del mantenimiento de la seguridad en los dispositivos móviles y la provisión del adecuado soporte técnico de seguridad para los usuarios.)
UBICACIÓN DE TRABAJO	En general, los riesgos de seguridad serán menores en aquellos dispositivos que se usen exclusivamente dentro del perímetro de seguridad del organismo, frente a aquellos otros que también puedan usarse en el exterior.
LIMITACIONES TÉCNICAS	Cuando es preciso ejecutar una concreta aplicación puede ser necesario usar determinado tipo de dispositivo móvil o sistema operativo. Este sería el caso, por ejemplo, que obligaría a usar un determinado tipo de dispositivo móvil o, más frecuentemente, un sistema operativo concreto (o una versión de tal sistema operativo), capaz de ejecutar el software cliente de gestión de seguridad de dispositivos móviles del organismo.
CONFORMIDAD CON LA NORMATIVA VIGENTE Y OTRAS REGULACIONES DE SEGURIDAD	Además de todo lo anterior, los organismos deberán asegurar que el uso de los dispositivos móviles en el seno de las competencias estatutarias que les corresponden se desarrolla en todo momento de conformidad con la legislación vigente: esquema nacional de seguridad, pero también la legislación sobre protección de datos de carácter personal, administración electrónica, firma electrónica y cualquier otra que resulte de aplicación.

Tabla 3. Factores a considerar a la hora de desarrollar la normativa de Seguridad en el uso de Dispositivos Móviles.

La aplicabilidad de cada uno de los factores anteriores vendrá determinada por la categoría de seguridad del sistema de información de que se trate. Así, aquellos organismos que, tras el pertinente análisis de riesgos, entiendan que el tratamiento de determinados datos comporta un riesgo singular, es probable que sólo admitan que el trabajo se desarrolle a través de dispositivos móviles debidamente securizados y

suministrados por la propia organización, exigiendo una autenticación robusta antes de permitir que el dispositivo acceda a los recursos corporativos sensibles.

Como las medidas de seguridad también pueden implantarse en los servidores, otro posible control de seguridad sería migrar los recursos de alto riesgo a servidores específicos, expresamente securizados, que deberán asumir la responsabilidad de la adecuada protección de los datos tratados.

Finalmente, en los casos más sensibles o de mayor riesgo, los organismos podrán decidir prohibir de manera absoluta de acceso a determinados tipos de información a través de dispositivos móviles de cualquier tipo.

En todo caso, a la vista de la evolución tecnológica, del incremento de las capacidades de los dispositivos móviles, de la efectividad de los controles de seguridad adoptados y de los diferentes tipos de amenazas para cada dispositivo o sistema operativo, los organismos deberán, periódicamente, acomodar su Normativa de Seguridad en el Uso de Dispositivos Móviles a estas nuevas realidades, re-considerando la tipología de dispositivos aceptados por la organización, los niveles de acceso requeridos en cada caso y, en su consecuencia, la disposición de las adecuadas medidas de seguridad.

Obviamente, la evolución tecnológica afectará también a los sistemas centralizados de gestión de dispositivos móviles (MDM), que los organismos deberán re-evaluar permanentemente.

Formación y concienciación de los usuarios

De forma análoga a lo que sucede con el equipamiento tradicional, los organismos deberán concienciar y formar a los usuarios respecto de la importancia de las medidas de seguridad adicionales deben adoptarse, así como de las responsabilidades de los usuarios respecto de la adopción de tales medidas y su mantenimiento.

Una de tales medidas sería limitar (o prohibir, en los casos más rigurosos) la constitución de redes inalámbricas personales (WPAN), tales como aquéllas que pueden construirse usando teclados o ratones inalámbricos, conectando los dispositivos o las impresoras de forma inalámbrica, sincronizando dispositivos de forma inalámbrica, o usando auriculares con micrófonos inalámbricos. Las tecnologías de base que suelen usarse para la construcción de estas redes incluyen Wi-Fi, Bluetooth y Near-Field Communications (NFC).

7.2 Desarrollo

Cuando el organismo ha redactado y aprobado su Normativa de Seguridad en el Uso de Dispositivos Móviles, ha identificado las necesidades operativas de tales dispositivos y ha completado las actividades señaladas en el punto anterior, el siguiente paso es determinar qué tipo de tecnologías de gestión de dispositivos móviles pueden usarse en el contexto de la organización, diseñando una solución para su despliegue.

Se trata, por tanto, de adoptar decisiones sobre consideraciones de seguridad de naturaleza eminentemente técnica. Entre las más importantes pueden citarse las señaladas en el cuadro siguiente.

CONSIDERACIONES DE SEGURIDAD DE NATURALEZA TÉCNICA	
ARQUITECTURA	Que debe incluir: - diseño de la arquitectura del servidor de gestión de Dispositivos móviles, especialmente a la hora de establecer Conexiones con los usuarios remotos (dmz, dlp, registro de Auditoría, etc.), primando aquellas arquitecturas que Otorguen control completo al organismo. - diseño de la arquitectura del software-cliente a instalar en Tales dispositivos. - determinación de la ubicación del servidor de gestión de Dispositivos móviles y del resto de los elementos Centralizados. - diseño de la arquitectura de las soluciones de red privada Virtual (vpn) que se precisen.
AUTENTICACIÓN	Selección de los métodos de autenticación de los usuarios y/o Dispositivos, incluyendo los procedimientos de asignación y Eliminación de autenticaciones, que, en su caso, deberá Contemplar su integración con los sistemas de autenticación Corporativos. Presencia de un servidor de autenticación en el lado servidor, en El que la suspensión y revocación de derechos y privilegios sea Instantánea.
CRIPTOGRAFÍA	Selección de los algoritmos de cifrado y protección de la Integridad de las comunicaciones de los dispositivos móviles, así Como determinación de la fortaleza y longitud de las claves Criptográficas.
REQUERIMIENTOS	Determinación de los estándares de seguridad mínimos para los Dispositivos móviles
APROVISIONAMIENTO DE DISPOSITIVOS	Determinación de los métodos que se emplearán para cargar en Los dispositivos móviles desplegados (tanto nuevos como viejos) El software-cliente, los autenticadores, opciones de configuración etc.
REQUERIMIENTOS DE CERTIFICACIÓN DE APLICACIONES.	Determinación de los requisitos de seguridad y funcionalidad Que las aplicaciones deben poseer, señalando los indicadores de cumplimiento que se usarán.

Tabla 4. Consideraciones de seguridad de naturaleza técnica.

Los aspectos de seguridad del diseño de la solución para dispositivos móviles deberán estar documentados en la planificación de la Seguridad Móvil del organismo.

Análogamente, el organismo deberá determinar cómo deberán tratarse de los incidentes de seguridad que involucren a dispositivos móviles, su gestión y documentación.

7.3 Implantación

Como hemos dicho, antes de desplegar definitivamente una solución en el organismo, conviene implantar previamente un proyecto piloto, contemplando la problemática más significativa analizada en la fase de Iniciación.

La evaluación del proyecto piloto comprenderá el análisis de, entre otros, los siguientes extremos:

ELEMENTOS A ANALIZAR EN LA IMPLANTACIÓN DEL PROYECTO-PILOTO	
CONECTIVIDAD	Establecimiento y mantenimiento por parte de los usuarios de conexiones al organismo desde aquellas ubicaciones que se espera sean usados. Dependiendo de los privilegios de acceso, los usuarios podrán Acceder a la totalidad de los recursos corporativos o solamente a cierto número de ellos.
PROTECCIÓN	Garantía de que la información almacenada en el dispositivo móvil y Las comunicaciones entre tal dispositivo y el organismo están Protegidas debidamente, de acuerdo con lo señalado en la Normativa de seguridad en el uso de dispositivos móviles del organismo.
AUTENTICACIÓN	Garantía de que no es posible circunvalar la autenticación de Usuario/dispositivo, cuando se trata de una exigencia determinada Por el nivel de acceso que se posea. Este aspecto requerirá la Evaluación de las políticas de autenticación de dispositivos, usuarios Y dominios.
APLICACIONES	Garantía de que las aplicaciones que habrán de ser ejecutadas en los dispositivos móviles funcionan adecuadamente. Este aspecto Requerirá la evaluación de las restricciones o limitaciones para la Instalación de aplicaciones, de manera especial las limitaciones para Desinstalar el software-cliente de gestión de dispositivos móviles del organismo.
GESTIÓN	Garantía de que los administradores del sistema (y los Administradores de seguridad) pueden configurar y gestionar todos Los componentes de la solución de manera efectiva y segura. Habrá De tenerse especialmente en cuenta la facilidad para el despliegue y La configuración de la solución, así como la imposibilidad o Dificultad de los usuarios para modificar la configuración del

	Software-cliente o del dispositivo.
LOGGING	Garantía de que la solución que finalmente se adopte mantiene un Log de eventos de seguridad, de acuerdo con la normativa de Seguridad en el uso de dispositivos móviles del organismo.
RENDIMIENTO	Garantía de que todos los componentes de la solución que Finalmente se adopte mantienen un rendimiento adecuado durante Un uso normal.
SEGURIDAD DE LA IMPLANTACIÓN	Como quiera que la solución adoptada pueda contener Vulnerabilidades que podrían ser explotadas por eventuales Atacantes, aquellos organismos que posean sistemas de información Categorizados con los niveles medio y alto deberán realizar una Valoración amplia de las vulnerabilidades de la solución que se Pretende adoptar. En todo caso, como requerimiento mínimo, Todos los componentes de la solución deberán estar actualizados Con los últimos parches disponibles, y configurados siguiendo lo Dispuesto en la normativa de seguridad en el uso de dispositivos Móviles del organismo. El organismo, además, deberá adoptar las Medidas necesarias para prevenir que un usuario pueda circunvalar Las características de seguridad de los dispositivos móviles, Incluyendo la detección automática de incumplimientos, cuando Ello sea posible, y la prohibición del uso de dispositivos *rooteados*.
CONFIGURACIÓN PREDETERMINADA	Garantía de que los valores de configuración por defecto de los Dispositivos móviles y/o su modificación son necesarios para Soportar los requisitos de seguridad definidos en la normativa de Seguridad en el uso de dispositivos móviles del organismo.

Tabla 5. Elementos a analizar en la implantación del proyecto de Seguridad en Dispositivos Móviles.

Como es lógico, el organismo debe securizar cada dispositivo móvil que entregue a los usuarios antes de permitir el acceso a los recursos corporativos. Esta cautela debe aplicarse igualmente para aquellos dispositivos móviles que ya hubieren sido desplegados por la organización. Además, dependiendo de los riesgos, podrán incorporarse al dispositivo determinados controles de seguridad adicionales, tales como software antivirus y tecnologías de prevención de pérdida de datos (Data Loss Prevention, DLP).

7.4 Operación y Mantenimiento

El cuadro siguiente enumera los procedimientos operativos más usuales que, de forma periódica, deben ser llevados a cabo por el organismo de que se trate, al objeto de mantener la seguridad de la infraestructura móvil desplegada en la organización.

P1	Verificación del estado de actualización y parcheado de los componentes de la solución para dispositivos móviles desplegada en el organismo, (contemplando mecanismos de adquisición, pruebas y despliegue de las actualizaciones), incluyendo los componentes de la infraestructura, los sistemas operativos de los dispositivos móviles y las aplicaciones contenidas en ellos.
P2	Verificación de que cada componente de la infraestructura de dispositivos móviles desplegada en el organismo (servidores de gestión de dispositivos móviles, servidores de autenticación, etc.) Está adecuadamente sincronizada usando una fuente de tiempo común confiable, que posibilite detectar sellos de tiempo generados por otros sistemas.
P3	Configurar las características de control de accesos en función de las necesidades generados por otros sistemas. Competenciales del usuario/dispositivo y sustentadas en factores tales como cambios en la política de seguridad, cambios tecnológicos, resultados de auditorías y nuevas necesidades de seguridad.
P4	Monitorizar de manera constante la infraestructura de dispositivos móviles del organismo, de manera que permita detectar y documentar incidentes y anomalías, incluyendo cambios de configuración no autorizados en los dispositivos móviles. Los incidentes de seguridad deben reportarse al sistema de gestión de incidentes de seguridad de los sistemas de información del organismo.
P5	Mantener un inventario actualizado de los dispositivos móviles desplegados en el organismo, incluyendo: su(s) usuario(s), las aplicaciones que contienen y los recursos corporativos a los que les está permitido acceder.
P6	Proporcionar formación a los usuarios de dispositivos móviles del organismo en relación con las amenazas de seguridad, incluyendo actividades de concienciación y la adopción de buenas prácticas.
P7	Revocar el acceso (o proceder al borrado) de aquellas aplicaciones, que habiendo sido ya instaladas en los dispositivos móviles, fueran evaluadas como de alto riesgo.
P8	Borrado seguro de todos los datos contenidos en los dispositivos móviles antes de permitir su reutilización por otros usuarios.
P9	Verificación periódica de cara a confirmar que las políticas de seguridad de dispositivos móviles del organismo, su normativa de desarrollo y sus procedimientos asociados están siendo seguidas adecuadamente por todos los usuarios. Tal verificación puede desarrollarse usando medios pasivos (revisión de logs, por ejemplo) o medios activos (tales como pruebas de penetración –ips- y de explotación de vulnerabilidades, etc.)

Tabla 6. Procedimientos para manterner la seguridad en la infraestructura móvil de la organización.

7.5 Retirada

Como se ha insistido, antes de que un componente de la infraestructura móvil desplegada en el organismo sea retirado permanentemente o reasignado a otro usuario57, la organización debe eliminar de manera segura y permanente cualquier dato o información sensible que todavía pudiera residir en los dispositivos móviles o, en general, en cualquier componente de la infraestructura desplegada.

Estas acciones de borrado seguro (como las que se realizan con los discos de estado sólido o las tarjetas de memoria, por ejemplo) comportan, en ocasiones, cierta dificultad, debido especialmente a la persistencia de datos de las memorias flash, lo que exige la utilización de procedimientos de borrado específicos para tal tipo de dispositivos.

Fuente capitulo [ENS]

Capítulo 8

Auditoría de Seguridad Informática

La Auditoría Informática es definida por ISACA como cualquier revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes. Debe entenderse como una herramienta más que ayudará a las organizaciones a supervisar su sistema de control e incluso a gesitonar sus riesgos, controlando además el equilibrio entre riesgos y costes de seguridad contra la eficacia del sistema.

la manera de hacerlo es regoger, agrupar y evaluar evidencias para determinar si un sistema de información:.

- Salvaguarda los activos.
- Mantiene la integridad de los datos.
- Lleva a cabo eficazmente los fines de la organización.
- Hace un buen uso de los recursos.
- Cumple con las leyes y regulaciones establecidas.

Para proceder, se realizan una serie de controles que evalúan las entradas al sistema de información, los procedimientos, la seguridad existente etc. Fianlmente, como resultado, a la empresa se le aportará una información válida, exacta, completa, actualizada y oportuna que ayude a ala toma de decisiones teniendo en cuenta los valores de calidad, plazo y coste.

8.1 Tipos de Auditoría

Según quien lleva a cabo la auditoría esta puede ser:

- **Interna**: Se caracteriza porque los recursos y personas pertenecen a la empresa u organización auditada, siendo por tanto la propia organización es la que lleva el control.
- **Externa**: Se caracteriza porque los recursos y personas no pertenecen a la empresa auditada. Sulen tener una mayor objetividad al no ser los mismos los auditores y los auditados

8.2 Principales Auditorías Informáticas

- **Auditoría del desarrollo**. Revisión de la metodología de desarrollo, control interno de las aplicaciones, satisfacción de usuarios, control de procesos y ejecuciones de programas críticos.
- **Auditoría de bases de datos.** Revisión de los controles de acceso, de actualización, de integridad y calidad de los datos.
- **Auditoría de sistemas.** Revisión de las medidas de seguridad de los sistemas operativos, optimización de los sistemas, etc.
- **Auditoría de la seguridad.** Referidos a datos e información verificando disponibilidad, integridad, confidencialidad, autenticación y no repudio.
- **Auditoría de redes**. Revisión de la topología de red y determinación de posibles mejoras, análisis de caudales y grados de utilización.
- **Auditoría de aplicaciones.**
  - Evaluar la eficiencia y efectividad de los sistemas de información que respalden los procesos de negocio.
  - Evaluar el diseño y la implementación de los controles programados y manuales para asegurar que los riesgos identificados para los procesos del negocio estén en un nivel aceptable.
  - Mitigar los riesgos de índole económica, de incumplimiento del marco legal y la normativa establecida y de falta de integridad de la información remitida a clientes
- **Auditorías de migración de aplicaciones**. Consiste en verificar los procedimientos y pruebas que se han realizado en los sistemas para verificar que la información del sistema antiguo y actual es la misma.
- **Auditoría de la gestión.** la contratación de bienes y servicios, documentación de los programas, etc.
- **Auditorías legales o de cumplimiento (LOPD, RD 1720/2007, SOX, ISO27001, ISO20000, ISO 9001).**
- **Auditoría de planes de contingencia y continuidad.**

  - Los planes deben estar formalizados por escrito y aprobados por la dirección.
  - Los empleados deben tener asignadas responsabilidades para su ejecución, las conocen y están preparados para realizarlas.
  - Deben abarcar todos los ámbitos críticos de la empresa y que en función de dicho aspecto se ha establecido el orden de prioridad en la recuperación.
  - Garantizar su actualización mediante revisiones y pruebas periódicas.

- **Auditoría de datos masivos**. Consiste en realizar mediante pruebas informáticas con herramientas de tratamiento masivo de datos (IDEA, ACL) para verificar que los cálculos automáticos de las aplicaciones se están realizando correctamente.
- **Auditorías físicas.** Revisión de la protección del hardware y de los soportes de datos, así como la de los edificios e instalaciones que los albergan, contemplando las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc. Para garantizar la integridad de los activos humanos, lógicos y material de un CPD.
- **Auditoría de servicios externalizados de TI**. Se trata de realizar auditorías a los proveedores externos donde se tienen externalizados los servicios para comprobar que estos se están realizando con la misma o mayor calidad que si fuesen realizados internamente y que están cumpliendo con lo establecido en los acuerdos de nivel de servicio.
- **Test de penetración o hacking ético.** Se trata de una penetración controlada en los sistemas informáticos de una empresa, de la misma forma que lo haría un hacker o pirata informático pero de forma ética.

8.3 ¿Por qué es importante realizar una auditoría informática?

La Auditoría Informática, es importante en las organizaciones auditadas por lo siguiente:

- Se puede dar o utilizar información errónea si la calidad de datos de entrada es inexacta o estos son manipulados.
- Los ordenadores, servidores y los Centros de Procesamiento de Datos se han convertido en blancos para fraudes, espionaje, delincuencia y terrorismo informático.
- La continuidad de las operaciones, la administración y organización de la empresa no deben residir en sistemas mal diseñados, ya que los mismos pueden convertirse en un serio peligro para la empresa.
- Las bases de datos pueden ser propensas a ataques y accesos de usuarios no autorizados o intrusos.

- La piratería de software y el uso no autorizado de programas, con las implicaciones legales y respectivas sanciones que esto puede tener para la empresa.
- El robo de secretos comerciales, información financiera, administrativa, la transferencia ilícita de tecnología y demás delitos informáticos.
- Mala imagen e insatisfacción de los usuarios porque no reciben el soporte técnico adecuado o no se reparan los daños de hardware ni se resuelven los problemas en plazos razonables, es decir, el usuario percibe que está abandonado y desatendido permanentemente.
- En el Departamento de Sistemas se observa un incremento desmesurado de costos, inversiones injustificadas o desviaciones presupuestarias significativas.
- Evaluación de nivel de riesgos en lo que respecta a seguridad lógica, seguridad física y confidencialidad.
- Mantener la continuidad del servicio y la elaboración y actualización de los planes de contingencia para lograr este objetivo.
- Los recursos tecnológicos de la empresa incluyendo instalaciones físicas, personal subalterno, horas de trabajo pagadas, programas, aplicaciones, servicios de correo, Internet, o comunicaciones; son utilizados por el personal sin importar su nivel jerárquico, para asuntos personales, alejados totalmente de las operaciones de la empresa o de las labores para las cuales fue contratado.
- El uso inadecuado del ordenador para usos ajenos de la organización, por ejemplo la copia de programas para fines de comercialización sin reportar los derechos de autor, o utilización de Internet de forma abusiva.

(Extraido de shellsec)

8.4 ¿Cómo debe ser el personal que compone una unidad de auditoría SI?

Formación: Aunque muchos de los profesionales con más antigüedad en este ámbito son titulados en especialidades relacionadas con la economía o el derecho, dada la naturaleza del trabajo del auditor de SI es adecuado que su formación esté relacionada con las TI, por ejemplo ingenieros informáticos o de telecomunicaciones. Además son valorables las certificaciones como CISA, CIA, CISSP, CISM, en estándares ISO, etc.

Trato con personas: Ya que a menudo la actividad del auditor es analizar y evaluar actividades realizadas por otras personas de la organización y que además tienen gran experiencia en su trabajo es muy importante que las personas que realizan los trabajos de auditoría sean capaces de:

- Ser empáticos, capaces de colocarse en la posición de la persona auditada.
- Posean capacidad para escuchar.
- Capacidad de negociación.
- Paciente, prudente y flexible.
- Con capacidad para defender sus puntos de vista.

Desarrollo del trabajo: Un auditor de SI debe ser ordenado, metódico y con gran capacidad de análisis y de síntesis. Debe saber trabajar en equipo y tener adecuadas habilidades para la redacción de informes y papeles de trabajo.

Honesto y reservado: debe mantener una conducta ética adecuada, cumpliendo el código de ética de ISACA, especialmente si se posee la certificación CISA, el cual detallo a continuación y mantener una estricta cautela a la hora de divulgar información.

Los miembros y los poseedores de certificaciones de ISACA , según su pagina web, deberán:

1. Respaldar la implementación y promover el cumplimiento con estándares y procedimientos apropiados del gobierno y gestión efectiva de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de auditoría, control, seguridad y riesgos.

2. Llevar a cabo sus labores con objetividad, debida diligencia y rigor/cuidado profesional, de acuerdo con estándares de la profesión.

3. Servir en beneficio de las partes interesadas de un modo legal y honesto y, al mismo tiempo, mantener altos niveles de conducta y carácter, y no involucrarse en actos que desacrediten su profesión o a la asociación.

4. Mantener la privacidad y confidencialidad de la información obtenida en el curso de sus deberes a menos que la divulgación sea requerida por una autoridad legal.

Dicha información no debe ser utilizada para beneficio personal ni revelada a partes inapropiadas.

5. Mantener la aptitud en sus respectivos campos y asumir sólo aquellas actividades que razonablemente esperen completar con las habilidades, conocimiento y competencias necesarias

6. Informar los resultados del trabajo realizado a las partes apropiadas, incluyendo la revelación de todos los hechos significativos sobre los cuales tengan conocimiento que, de no ser divulgados, pueden distorsionar el reporte de los resultados.

7. Respaldar la educación profesional de las partes interesadas para que tengan una mejor comprensión del gobierno y la gestión de los sistemas de información y la tecnología de la empresa, incluyendo la gestión de la auditoría, control, seguridad y riesgos.

La certificación más importante que existe para acreditar la capacidad de un profesional para desempeñar o ejecutar labores de auditoría de sistemas es la certificación CISA realizada por ISACA desde 1978 tiene un gran prestigio. Por lo que todos los miembros del departamento deberían tener esta certificación.

Otras certificaciones relacionadas serian:

- CIA: promovida por el IIA (The Institute of Internal Auditors), que tiene gran reconocimiento para los profesionales de auditoría interna.
- CISSP: promovida por ISC y relacionada con la seguridad de los sistemas de información.
- CISM: promovida por ISACA y también relacionada con la seguridad de los sistemas de información.

La relacionada con los estándares ISO o británicos de seguridad de la información.

Capítulo 9

Legislación actual en España

En el presente capítulo, se recoge la situación legislativa presente en España, donde existen varias normas, que a continuación desglosaremos. Estas normas están relacionadas con las conductas y actividades ilícitas realizadas por medio de los distintos dispositivos tecnológicos como pueden ser ordenadores, smartphones, portátiles, tabletas, relojes. Es más, la gran proliferación de dispositivos con posibilidad de ser conectados a Internet hace que podamos incluso extendernos a televisiones, consolas de videojuegos, coches, aparatos de navegación etc, etc.

Aunque estos actos, conocidos también como delitos o fraudes informáticos, no están contemplados como un tipo especial de delito en la legislación española, existen varias normas relacionadas con este tipo de conductas:

- Ley Orgánica de Protección de Datos de Carácter Personal (LOPDCP).
- Real Decreto 1720/2007.
- Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI).
- Ley General de Telecomunicaciones.
- Ley de Propiedad Intelectual.
- Ley de Firma Electrónica.

9.1 Ley Orgánica 15/1999. Ley de Protección de Datos de Carácter Personal (LOPD)

La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD) supone una modificación importante del régimen sobre protección de datos de personas físicas contenido hasta entonces en la extinta LORTAD.

Tiene como objetivo regular, garantizar y proteger el uso que se hace de los datos personales imágenes, o videos de terceros y estipula fuertes multas en caso de que se atente contra el honor, la intimidad, la privacidad y los derechos fundamentales de las personas físicas.

A continuación se presenta el ámbito de aplicación de dicha ley:

1. La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado.

Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a. Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b. Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c. Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

2. El régimen de protección de los datos de carácter personal que se establece en la presente Ley Orgánica no será de aplicación:

a. A los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.

b. A los ficheros sometidos a la normativa sobre protección de materias clasificadas.

c. A los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

3. Se regirán por sus disposiciones específicas, y por lo especialmente previsto, en su caso, por esta Ley Orgánica los siguientes tratamientos de datos personales:

a. Los ficheros regulados por la legislación de régimen electoral.

b. Los que sirvan a fines exclusivamente estadísticos, y estén amparados por la legislación estatal o autonómica sobre la función estadística pública.

c. Los que tengan por objeto el almacenamiento de los datos contenidos en los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.

d. Los derivados del Registro Civil y del Registro Central de penados y rebeldes.

e. Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad, de conformidad con la legislación sobre la materia.

9.2 Real Decreto. 1720/2007

El reglamento viene a abarcar el ámbito tutelado anteriormente por la Ley Orgánica de Protección de Datos, teniendo en cuenta la necesidad de fijar criterios aplicables a los ficheros y tratamientos de datos personales no automatizados. Por otra parte, la atribución de funciones a la Agencia Española de Protección de Datos por la Ley 34/2002, de 11 de julio, de Servicios de la sociedad de la información y de comercio electrónico y la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, que más tarde comentaremos, obliga a desarrollar también los procedimientos para el ejercicio de la potestad sancionadora por la Agencia.

El reglamento se estructura en nueve títulos cuyos contenidos desarrollan los aspectos siguientes:

El título I contempla el objeto y ámbito de aplicación del reglamento. Se ha advertido la conveniencia de desarrollar el apartado 2 de su artículo 2 para aclarar qué se entiende por ficheros y tratamientos relacionados con actividades personales o domésticas, aspecto muy relevante dado que están excluidos de la normativa sobre protección de datos de carácter personal.

Además, en este título se aporta un conjunto de definiciones que ayudan al correcto entendimiento de la norma, lo que resulta particularmente necesario en un ámbito tan tecnificado como el de la protección de datos personales. Por otra parte, fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar esta cuestión evitando distinciones que suponen diferencias de trato de los ficheros públicos respecto de los privados.

El título II, se refiere a los principios de la protección de datos. Reviste particular importancia la regulación del modo de captación del consentimiento atendiendo a aspectos muy específicos como el caso de los servicios de comunicaciones electrónicas y, muy particularmente, la captación de datos de los menores. Las previsiones en este ámbito se completan con lo dispuesto en el título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.

El título III se ocupa de una cuestión tan esencial como los derechos de las personas en este ámbito. Estos derechos de acceso, rectificación, cancelación y oposición al tratamiento, constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho

fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

A continuación, los títulos IV a VII permiten clarificar aspectos importantes para el tráfico ordinario, como la aplicación de criterios específicos a determinado tipo de ficheros de titularidad privada que por su trascendencia lo requerían -los relativos a la solvencia patrimonial y crédito y los utilizados en actividades de publicidad y prospección comercial

El título VIII regula un aspecto esencial para la tutela del derecho fundamental a la protección de datos, la seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y aún de inversión, en todas las organizaciones que traten datos personales.

Finalmente en el título IX, dedicado a los procedimientos tramitados por la Agencia Española de Protección de Datos, se recogen exclusivamente aquellas especialidades que diferencian a los distintos procedimientos tramitados por la Agencia de las normas generales previstas para los procedimientos en la ley.

9.3 Ley 34/2002, de 11 de julio. Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSICE)

La LSSICE supone la primera regulación legal que con carácter general se dicta en España para el entorno de Internet. Sus principales objetivos consisten en:

1. Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.

2. Las disposiciones contenidas en esta Ley se entenderán sin perjuicio de lo dispuesto en otras normas estatales o autonómicas ajenas al ámbito normativo coordinado, o que tengan como finalidad la protección de la salud y seguridad pública, incluida la salvaguarda de la defensa nacional, los intereses del consumidor, el régimen tributario aplicable a los servicios de la sociedad de la información, la protección de datos personales y la normativa reguladora de defensa de la competencia

9.4 Ley 32/2003 de 3 de noviembre. Ley General de Telecomunicaciones

La Ley General de Telecomunicaciones persigue garantizar el cumplimiento de los objetivos de la Agenda Digital para Europa, que requiere, en la actual situación de evolución tecnológica e incertidumbre económica, asegurar un marco regulatorio claro y estable que fomente la inversión, proporcione seguridad jurídica y elimine las barreras que han dificultado el despliegue de redes, y un mayor grado de competencia en el mercado.

Para ello, con fundamento en la competencia exclusiva estatal en materia de telecomunicaciones del artículo 149.1.21.ª de la Constitución y en las competencias de carácter transversal de los artículos 149.1.1.ª y 149.1.13.ª del texto constitucional, la Ley persigue, como uno de sus principales objetivos, el de recuperar la unidad de mercado en el sector de las telecomunicaciones, estableciendo procedimientos de coordinación y resolución de conflictos entre la legislación sectorial estatal y la legislación de las Administraciones competentes dictada en el ejercicio de sus competencias que pueda afectar al despliegue de redes y a la prestación de servicios.

Con el objetivo de facilitar el despliegue de redes y la prestación de servicios de comunicaciones electrónicas, se procede a una simplificación administrativa, eliminando licencias y autorizaciones por parte de la administración de las telecomunicaciones para determinadas categorías de instalaciones que hacen uso del espectro. En la misma línea se prevé una revisión de las licencias o autorizaciones por parte de las Administraciones competentes, eliminando su exigibilidad para determinadas instalaciones en propiedad privada o para la renovación tecnológica de las redes y se facilita el despliegue de las nuevas redes permitiendo el acceso a las infraestructuras de otros sectores económicos susceptibles de ser utilizadas para el despliegue de redes de comunicaciones electrónicas.

En esta misma línea de reducción de cargas administrativas, la Ley simplifica las obligaciones de información de los operadores, a los que únicamente se les podrá solicitar aquella información que no se encuentre ya en poder de las Autoridades Nacionales de Reglamentación.

Asimismo, se establecen condiciones estrictas para la existencia de operadores controlados directa o indirectamente por administraciones públicas, de manera que, fuera del concepto de autoprestación, se garantice la provisión de los servicios bajo condiciones de mercado y criterios de inversor privado, evitando de este modo que se produzcan distorsiones de la competencia, y con el objetivo de racionalizar el gasto público.

La Ley incorpora, asimismo, las previsiones recogidas en la Ley 3/2013, de 4 de junio, de creación de la Comisión Nacional de los Mercados y de la Competencia, atribuyendo en todo caso a dicha Comisión las competencias de regulación y resolución de conflictos entre operadores reconocidas por la normativa comunitaria.

Por último, como necesario contrapunto a la reducción de las cargas y obligaciones impuestas a los operadores, la Ley refuerza el control del dominio público radioeléctrico y las potestades de inspección y sanción, facilitando la adopción de medidas cautelares y revisando la cuantía de las sanciones.

En definitiva, los criterios de liberalización del sector, libre competencia, de recuperación de la unidad de mercado y de reducción de cargas que inspiran este texto legal pretenden aportar seguridad jurídica a los operadores y crear las condiciones necesarias para la existencia de una competencia efectiva, para la realización de inversiones en el despliegue de redes de nueva generación y para la prestación de nuevos servicios, de modo que el sector pueda contribuir al necesario crecimiento económico del país.

9.5 Real Decreto Legislativo 1/1996, de 12 de abril (BOE 22-4-1996), por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual

La Ley de Propiedad Intelectual aclara y armoniza las disposiciones legales vigentes sobre el software pirateado, es decir sobre aquellos programas, excluyendo los gratuitos y libres, que se utilizan sin haber pagado previamente su licencia de uso.

9.6 Real Decreto Legislativo 14/1999, de 17 de septiembre, sobre Firma Electrónica

1. Este Real Decreto-Ley regula el uso de la firma electrónica, el reconocimiento de su eficacia jurídica y la prestación al público de servicios de certificación. Las normas sobre esta actividad son de aplicación a los prestadores de servicios establecidos en España.

2. Las disposiciones contenidas en este Real Decreto-Ley no alteran las normas relativas a la celebración, la formalización, la validez y la eficacia de los contratos y otros actos jurídicos ni al régimen jurídico aplicable a las obligaciones.

Las normas sobre la prestación de servicios de certificación de firma electrónica que recoge este Real Decreto-Ley no sustituyen ni modifican las que regulan las funciones que corresponde realizar a las personas facultadas, con arreglo a derecho, para dar fe de la firma en documentos o para intervenir en su elevación a públicos.

9.7 Legislación adicional

Existen numerosas leyes adicionales que versan sobre la regulación de la seguridad de la Información, centrándose en aspectos tales como la privacidad y la protección de la intimidad de los usuarios. A continuación se exponen las principales leyes, para poder dar una mayor completitud al ámbito legislativo que engloba todos los comportamientos registrados como delitos en el Código Penal español, con el fin de poder adoptar comportamientos útiles legalmente en caso de delito.

Las que más se aproximan se reflejan en los siguientes artículos:

Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos:

- El Artículo 197 contempla las penas con las que se castigará:
  - ✓ A quien, con el fin de descubrir los secretos o vulnerar la intimidad de otro, se apodere de cualquier documentación o efecto personal, intercepte sus telecomunicaciones o utilice artificios de escucha, transmisión, grabación o reproducción de cualquier señal de comunicación.
  - ✓ A quien acceda por cualquier medio, utilice o modifique, en perjuicio de terceros, a datos reservados de carácter personal o familiar, registrados o almacenados en cualquier tipo de soporte.
  - ✓ Si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.
- En el artículo 278.1 se exponen las penas con las que se castigará a quien lleve a cabo las mismas acciones expuestas anteriormente, pero con el fin de descubrir secretos de empresa.
- El Artículo 264.2 trata de las penas que se impondrán al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Delitos informáticos:

- Los artículos 248 y 249 tratan las estafas. En concreto el artículo 248.2 considera las estafas llevadas a cabo mediante manipulación informática**.**
- A día de hoy, las leyes se van adaptando poco a poco a las nuevas situaciones y escenarios que se presentan en el ámbito tecnológico, de tal forma que su cometido es ir poniendo límites y acotando las artificios semejantes.
- Los artículos 255 y 256 mencionan las penas que se impondrán a quienes cometan defraudaciones utilizando, entre otros medios, las telecomunicaciones.

Delitos relacionados con el contenido:

- El artículo 186 cita las penas que se impondrán a aquellos, que por cualquier medio directo, vendan, difundan o exhiban material pornográfico entre menores de edad o incapaces.
- El artículo 189 trata las medidas que se impondrán a quien utilice a menores de edad o a incapaces con fines exhibicionistas o pornográficos, y quien produzca, venda, distribuya, exhiba o facilite la producción, venta, distribución o exhibición de material pornográfico, en cuya elaboración se hayan utilizado menores de edad o incapaces.

Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: El Artículo 270 recopila las penas con las que se castigará a quienes reproduzcan, distribuyan o comuniquen públicamente, una parte o la totalidad, de una obra literaria, artística o científica, con ánimo de lucro y en perjuicio de terceros.

- El artículo 273 trata las penas que se impondrán a quienes sin consentimiento del titular de una patente, fabrique, importe, posea, utilice, ofrezca o introduzca en el comercio, objetos amparados portales derechos, con fines comerciales o industriales.

Existen nuevas amenazas que pueden irse presentando día a día al usuario de cualquier tipo de tecnología informática. Evidentemente, la ley siempre irá un paso por detrás de los infractores que utilicen las nuevas tecnologías para perjudicar a los usuarios, pero el esfuerzo de los cuerpos legislativos del Estado se centra en mantener un estrecho cerco a estos infractores, así como perseguir y denunciar los nuevos métodos que éstos vayan implementando para cometer los fraudes y estafas.

Así, algunas conductas como el spam (envío de publicidad no deseada, normalmente a través del correo electrónico) no estaban contempladas entre los delitos tipificados en el Código penal español, pero esta actividad ya ha sido incorporada en la LSSI de tal forma que actualmente ya es imputable este tipo de actividades. Como vemos, la legislación va avanzando y amoldándose a todas estas nuevas tecnologías, pero como siempre, el problema reside en que primero han de ocurrir reiteradamente estos "nuevos delitos" para que posteriormente sean reflejados en la legislación española.

Fuentes consultadas:

- ***itsinformatica.com/legislacion.html#lpi***
- ***www.agdp.es*** [AGDP]

Capítulo 10

Diseño de aplicación

En este apartado se mostrará el prototipo de una aplicación pensada para medir cuan de seguro es un determinado sistema.

10.1 Objetivo de la aplicación

El objetivo de la aplicación sería poder llevar a cabo una pre-auditoria sobre el cumplimiento de las políticas de seguridad en un determinado entorno (1 – n dispositivos/ aplicaciones). Para ello las aplicaciones, o dispositivos a verificar serán sometidas a unos determinados controles y tras valorar los resultados obtenidos se presentará el grado de cumplimiento con la normativa cotejada.

De aquí en adelante a nuestro prototipo le llamaremos CPS. El nombre surge del objetivo de la aplicación, realizar un control sobre el cumplimiento de las políticas de seguridad de la organización: “Control Políticas de Seguridad”

10.2 Inicio del Ciclo

La idea está pensada para que la aplicación se utilice de manera constante e incluso periódica. Y su fin no es auditar una sola aplicación en un determinado periodo de tiempo, su fin es poder auditar varias a la vez. Esta destinada a organizaciones con el fin de tener un boceto de cómo de alineada esta una organización con unas determinadas políticas de seguridad como pueden, por ejemplo, ser: la ISO 27002, la ley SOX, la LOPD, etc.

Por tanto, al comenzar un nuevo ciclo, el primer paso será delimitar el ámbito, es decir todos los componentes que queremos analizar, el paso siguiente es darlo de alta en la plataforma de gestión del servicio

Figura 4. Ejemplo del menú desde el que se configura el ciclo a analizar

En un menú similar a este se indicarían todos los parámetros necesarios para definir el ciclo que comienza. Por ejemplo, aquí se indicará la fecha de inicio, fecha de fin, y una breve descripción del mismo.

Los controles que se verificaran en cada uno de los componentes dados de alta ya estarán previamente definidos en la herramienta CPS, no obstante siempre tendremos la posibilidad de poder crear nuevos o eliminar los que no nos interesen como se verá a continuación.

Figura 5. Ejemplo de pantalla de alta de ciclo

10.2.1 Crear/Modificar/Borrar – poblaciones/controles a auditar

Para sucesivos ciclos el proceso de creación de ciclo tomará por defecto las poblaciones o componentes a analizar y los controles del ciclo anterior, por tanto, como ya hemos adelantado se debe de realizar un proceso manual en la plataforma en el que se crea/modifica/borra las poblaciones/controles oportunas para adaptarlo al ámbito del nuevo ciclo.

Figura 6. Ejemplo del menú y del submenú desde donde se configura el ciclo a analizar

10.2.2 Definir controles.

Al comienzo de cada uno de los ciclo se debe de llevar a cabo la definición de los controles a los que se va a someter el activo a analizar. Estos controles suelen permanecer estáticos entre ciclos, a no ser que haya alguna incorporación de subcontroles nuevos, o alguna modificación en los ya existentes.

10.3 Recolección de datos.

Todo aquello que no se pueda verificar de forma automática se verificará mediante cuestionarios. Por tanto la recolección de datos se llevará a cabo tanto de forma automática mediante scripts como de forma manual mediante cuestionarios.

10.3.1 Cuestionarios Manuales (Montaje/Envío/Recepción)

Montaje de cuestionarios

Se realiza un cuestionario por cada una de las aplicaciones, este cuestionario es un fichero excel, que contiene una pestaña por cada una de las capas que le apliquen:

- Capa Organizativa: Con preguntas que tienen que ver con la organización o empresa donde se lleva a cabo la utilización de la herramienta.
- Capa de Aplicación: Con preguntas relacionadas al activo como aplicación, es decir cuando el usuario la utiliza a través de una interfaz.
- Capa de SSOO: Contendrá todas aquellas preguntas que tengan que ver con el Sistema Operativo donde corre el activo analizado.
- Capa de BBDD: Si detrás del activo se encuentra una base de datos respaldando la aplicación.

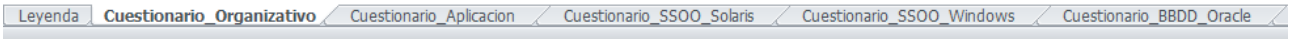


Figura 7. Pestañas de cuestionario

Así pues, cada pestaña consta de una serie de subcontroles con sus correspondientes preguntas, las cuales serán contestadas por el responsable del activo o de la capa del activo.

<Nombre de Aplicación> <Capa>

SUBCONTROL	PREGUNTAS ASOCIADAS	RESPUESTA	COMENTARIOS/EVIDENCIAS	CONFORMIDAD
DC1-C01-01	La Dirección debe aprobar un documento de Política de Seguridad de la Información, publicarlo y distribuirlo a todos los empleados y terceros afectados.			
	¿Esta aprobado por la dirección un documento de política o normativa de seguridad de la información?			
	¿Este documento esta publicado, accesible y distribuido a todos los empleados y terceros afectados?			
DC1-C01-02	El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente. Además, este documento será de obligado cumplimiento para el personal con acceso a los sistemas de información.			
	Los responsables de los ficheros o tratamiento, ¿tienen elaborado un documento de seguridad que recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente?			
	¿Este documento de seguridad es de obligado cumplimiento para el personal con acceso a los sistemas de seguridad?			
	¿Contiene los aspectos mínimos exigidos por el Reglamento?			
DC1-C01-03	El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes. Asimismo, el contenido de este documento deberá adecuarse a la normativa afín vigente en materia de seguridad de los datos de carácter personal.			
	¿Está el documento de seguridad actualizado?			
	¿se ha revisado cuando se han producido cambios relevantes desde la auditoría anterior?			
	¿Está su contenido adecuado a la normativa vigente en este momento en materia de seguridad de los datos de carácter personal?			

Figura 8. Ejemplo de cuestionario enviado

Envío de cuestionarios

La recopilación de datos manuales se realiza mediante cuestionarios que se emplearán en las entrevistas con los responsables identificados. Dichos cuestionarios se enviarán a los mismos vía correo electrónico previamente para facilitarles la preparación de las mismas. Este proceso se puede realizar de diferentes formas: en ocasiones se realiza un solo envío con el cuestionario completo al responsable, en otras ocasiones, el cuestionario se divide en partes, enviando cada parte al responsable o equipo de trabajo correspondiente.

Recepción de cuestionarios

Tras ser contestados los cuestionarios por parte de los diferentes responsables, estos son devueltos al grupo que realiza la pre-auditoria. Los cuestionarios son revisados para comprobar que todas las respuestas vienen cubiertas y no falta ningún documento o evidencia que apoye el cuestionario.

<Nombre de Aplicación> <Capa>

SUBCONTROL	PREGUNTAS ASOCIADAS	RESPUESTA	COMENTARIOS/EVIDENCIAS	CONFORMIDAD
DC1-C01-01	La Dirección debe aprobar un documento de Política de Seguridad de la Información, publicarlo y distribuirlo a todos los empleados y terceros afectados.	**Seguridad de la Información**		1
	¿Esta aprobado por la dirección un documento de política o normativa de seguridad de la información?	Sí, existe una política de seguridad aprobada por la dirección. En la BD de NOTES de normas, políticas y procedimientos.	Ruta al documento de seguridad.	
	¿Este documento esta publicado, accesible y distribuido a todos los empleados y terceros afectados?	Sí, la política esta accesible desde la intranet de Vodafone.		
DC1-C01-02	El responsable del fichero o tratamiento elaborará un documento de seguridad que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente. Además, este documento será de obligado cumplimiento para el personal con acceso a los sistemas de información.	**Seguridad de la Información**		1
	Los responsables de los ficheros o tratamiento, ¿tienen elaborado un documento de seguridad que recoge las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente?	Sí, existe el documento de seguridad corporativo.	Ruta al documento de seguridad.	
	¿Este documento de seguridad es de obligado cumplimiento para el personal con acceso a los sistemas de seguridad?	Sí.	Ruta al documento de seguridad.	
	¿Contiene los aspectos mínimos exigidos por el Reglamento?	Sí.	Ruta al documento de seguridad.	
DC1-C01-03	El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes. Asimismo, el contenido de este documento deberá adecuarse a la normativa afín vigente en materia de seguridad de los datos de carácter personal.	**Seguridad de la Información**		1
	¿Está el documento de seguridad actualizado?	Sí, se actualiza con periodicidad mensual mediante el procedimiento GDS de Seguridad de la Información. Se trabaja con un control de cambios y con periodicidad trimestral se revisa y se pasa a definitiva por parte de Seguridad de la Información.	Ruta al documento de seguridad.	

Figura 9. Ejemplo de cuestionario recibido

10.3.2 Scripts Automáticos (Montaje/Envío/Recepción)

Montaje de Scripts de recolección

Para la recolección de toda la parte automática es suficiente con ejecutar en los dominios correspondientes unos scripts que recogerán toda la información necesaria para llevar a cabo el proceso. Antes de enviar los scripts a los distintos responsables para que sean ejecutados en las máquinas y bases de datos en producción, estos son revisados, y si fuera necesario modificados (optimización del proceso, nuevos datos a recolectar, etc.) y probados (testeados en máquinas de pruebas).

```
#############################################################################
#
# Parametros de configuracion del script
#
#############################################################################

VERSION='1.0'
APP_PREFIX='vodasox'
TARGET='SunOS'

TMP_DIR='/var/tmp'
OUTPUT_DIR='/var/tmp'

USER_EXEC='vodasox'
USER_READ='vodasoxr'
GROUP='vodasox'
HOME_OUTPUT_PREFIX='output'

# Sufijo del fichero de carga de variables en entorno en comandos 'collect'
ENV_SUFFIX='.env.sh'

fecha=`date '+%Y%m%d%H%M%S'`
hostname=`hostname`
```

Figura 10. Script de recolección

Envío de Scripts de recolección

Para la recolección de los scripts hay dos formas de realizarlo:

- Apertura de una petición en la herramienta que la organización utilice, (por ejemplo Remedy) al equipo de administración correspondiente.

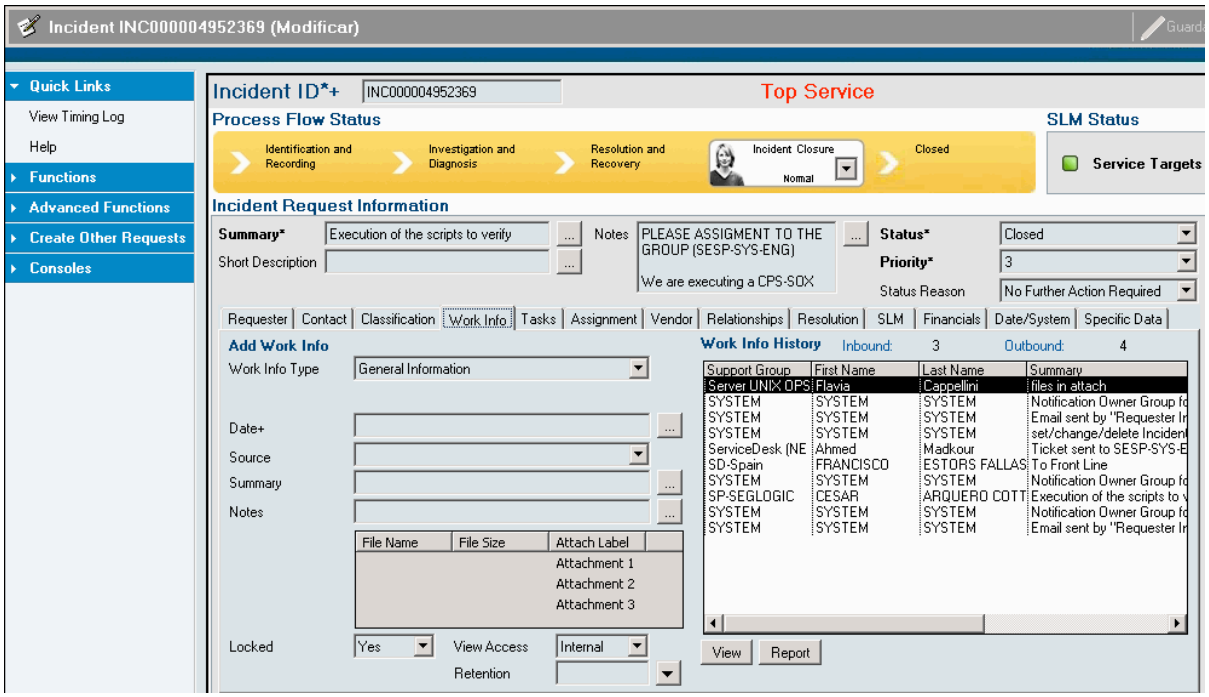
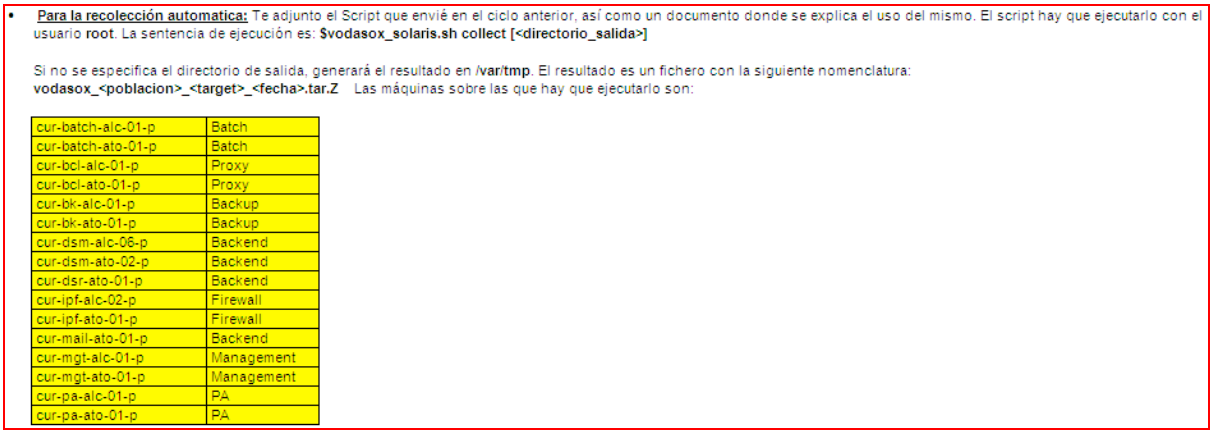


Figura 11. Ejemplo de apertura de una petición en Vodafone para le ejecución de un script

- Vía correo electrónico al responsable para cada una de las maquinas/bases de datos en las que hay que recolectar datos.



- **Para la recolección automatica:** Te adjunto el Script que envié en el ciclo anterior, así como un documento donde se explica el uso del mismo. El script hay que ejecutarlo con el usuario **root**. La sentencia de ejecución es: **$vodasox_solaris.sh collect [<directorio_salida>]**

Si no se especifica el directorio de salida, generará el resultado en **/var/tmp**. El resultado es un fichero con la siguiente nomenclatura: **vodasox_<poblacion>_<target>_<fecha>.tar.Z** Las máquinas sobre las que hay que ejecutarlo son:

cur-batch-alc-01-p	Batch
cur-batch-ato-01-p	Batch
cur-bcl-alc-01-p	Proxy
cur-bcl-ato-01-p	Proxy
cur-bk-alc-01-p	Backup
cur-bk-ato-01-p	Backup
cur-dsm-alc-06-p	Backend
cur-dsm-ato-02-p	Backend
cur-dsr-ato-01-p	Backend
cur-ipf-alc-02-p	Firewall
cur-ipf-ato-01-p	Firewall
cur-mail-ato-01-p	Backend
cur-mgt-alc-01-p	Management
cur-mgt-ato-01-p	Management
cur-pa-alc-01-p	PA
cur-pa-ato-01-p	PA

Figura 12. Ejemplo de correo electrónico con los script que deben ser ejecutados

Recepción Scripts de recolección

Dependiendo del método de envío, existirán dos formas de realizar la recepción de los scripts :

- Descargando los ficheros adjuntos de las correspondientes peticiones que se abrieron en la etapa de envío.

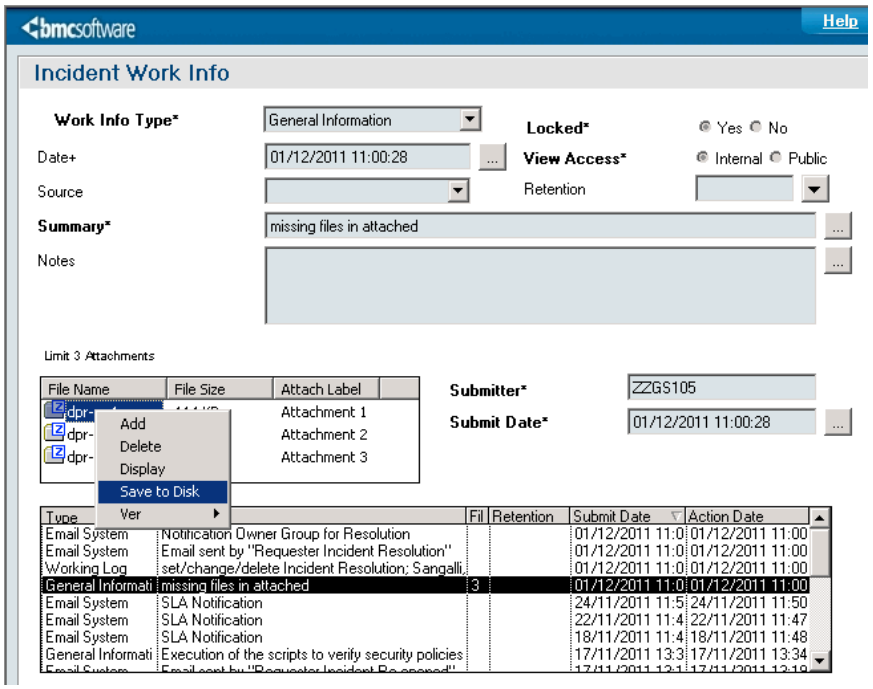


Figura 13. Ejemplo de recepción de datos recolectados a través de Remedy

- Descargando los ficheros adjuntos de los correos que se enviaron a los responsables en la etapa de envío.

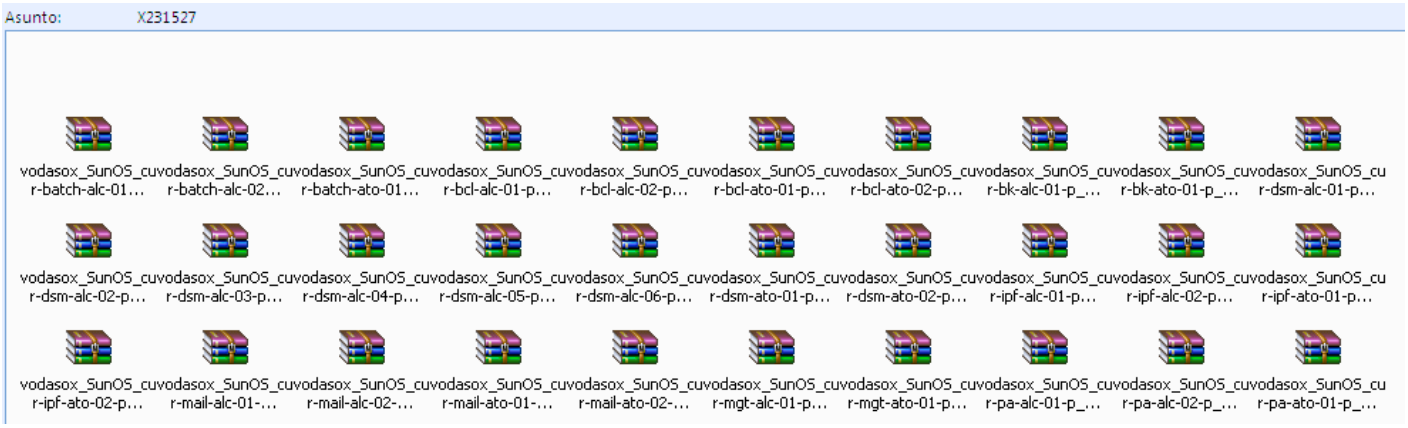


Figura 14. Ejemplo de datos recolectados a través del correo electrónico

En cualquiera de los dos casos anteriores es necesario revisar que los scripts vienen con sus datos correspondientes y que la fecha de ejecución es la del presente ciclo.

Para este proceso se utiliza una matriz de apoyo para identificar los ficheros necesarios para evaluar cada control.

Subcontrol	APP	Sybase	Oracle	HP-UX	Solaris	Windows
DC4-C01-12	Maestro_De_Usuarios.mdb Tablas auxiliares	Maestro_De_Usuarios.mdb Tablas auxiliares	Maestro_De_Usuarios.mdb Tablas auxiliares	Maestro_De_Usuarios.mdb Tablas auxiliares	Maestro_De_Usuarios.mdb Tablas auxiliares	Maestro_De_Usuarios.mdb Tablas auxiliares
DC4-C06-09	na	na	na	Maestro_De_Usuarios.mdb tmp\results\011_RunningProcesses.out tmp\results\009_DirzFullList.out tmp\files\etc\inetd.conf Tablas auxiliares /usr/sbin/nfsd (utilizacion NFS) (utilización SENDMAIL) /usr/sbin/rlpdaemon (utilización LP)	Maestro_De_Usuarios.mdb tmp\results\009_RunningProcesses.out tmp\results\007_DirzFullList.out tmp\files\etc\inetd.conf Tablas auxiliares /usr/sbin/nfsd (utilizacion NFS) (utilización SENDMAIL) /in.lpd (utilización LP)	na
DC4-C10-01	na	tmp\results\paramconfig.txt log audit logon failure log audit logon success	na	tmp\files\etc\syslog.conf tmp\files\var\adm\btmp tmp\files\var\adm\btmpx tmp\files\var\adm\btmps tmp\files\var\adm\wtmp tmp\files\var\adm\wtmpx tmp\files\var\adm\wtmps tmp \files\etc\utmp tmp\files\etc\utmpx tmp\files\etc\utmps Registro de los intentos de acceso correctos o incorrectos de usuarios	\files\etc\syslog.conf auth.notice security.notice	InfoSys1_SECEDIT AuditLogonEvents
DC4-C10-02	na	na	na	na	na	InfoSys1_SECEDIT AuditSystemEvents
DC5-C02-03	Maestro_De_Usuarios.mdb Maestro_SASI.mdb Tablas Auxiliares Tablas SASI	Maestro_De_Usuarios.mdb Maestro_SASI.mdb Tablas Auxiliares Tablas SASI	Maestro_De_Usuarios.mdb Maestro_SASI.mdb Tablas Auxiliares Tablas SASI	Maestro_De_Usuarios.mdb Maestro_SASI.mdb Tablas Auxiliares Tablas SASI	Maestro_De_Usuarios.mdb Maestro_SASI.mdb Tablas Auxiliares Tablas SASI	Maestro_De_Usuarios.mdb Maestro_SASI.mdb Tablas Auxiliares Tablas SASI
DC5-C02-09	na	na	na	tmp\files\var\adm\cron\cron.allow (opcional) tmp\files\var\adm\cron\cron.deny (opcional) Usuarios que pueden o no pueden usar cron	tmp\files\etc\cron.d\cron.allow (opcional) tmp\files\etc\cron.d\cron.deny (opcional) Usuarios que pueden o no pueden usar cron	na
DC5-C02-10	na	na	na	tmp\files\var\adm\cron\at.allow (opcional) tmp\files\var\adm\cron\at.deny (opcional) Usuarios que pueden o no pueden usar at	tmp\files\etc\cron.d\at.allow (opcional) tmp\files\etc\cron.d\at.deny (opcional) Usuarios que pueden o no pueden usar at	na
DC5-C02-11	na	na	na	tmp\files\etc\hosts.equiv (opcional) tmp\files\home (opcional) El fichero hosts.equiv no existe o está vacío. Los ficheros rhosts no existen o están vacíos	tmp\files\etc\hosts.equiv (opcional) tmp\files\home (opcional) El fichero hosts.equiv no existe o está vacío. Los ficheros rhosts no existen o están vacíos	na
DC5-C02-12	na	na	na	tmp\files\etc\passwd Solo un UID=0 y debe coincidir con root	tmp\files\etc\passwd Solo un UID=0 y debe coincidir con root	na

Figura 15. Ejemplo de matriz donde se muestra los archivos necesarios y recogidos por los script para poder llevar a cabo la verificación automática.

10.4 Verificación

10.4.1 Cuestionarios (Verificación/Carga en la plataforma)

Para llevar a cabo la verificación manual de cuestionarios se parte de la ficha correspondiente a cada uno de los controles. En estas fichas aparece indicado cómo o qué hay que mirar para verificar el control. Esta verificación se realiza sobre los cuestionarios rellenados en base a la información recogida mediante correos y/o sesiones de trabajo con los responsables de las poblaciones a verificar.

En los cuestionarios aparecerán las respuestas dadas por los responsables a las diferentes preguntas correspondientes a los controles.

El resultado de una verificación solo puede tener dos estados:

- **Verificación satisfactoria = 1**: El control se cumple.
- **Verificación no conforme = 0:** El control no se cumple.

DC4-C10-10	Los dispositivos de registro y la información de los registros deben estar protegidos contra manipulaciones indebidas y accesos no autorizados.	**Responsable**		**1**
	¿Están los dispositivos de registro, y la información de los registros"logs" protegidos contra manipulaciones indebidas y accesos no autorizados?	Sí, el unico usuario que tiene permisos para acceder a los ficheros de registro (logs) es el Root.		
DC4-C10-13	Se deben registrar las actividades del administrador del sistema y de la operación del sistema.	**Responsable**		**1**
	¿Se guarda el registro de la actividad que realizan los administradores y operadores del sistema?	Sí. Se guardan los comandos que los usuarios ejecutan. Se guardan en $HOME/.bash_history.	/etc/profile/ HISTFILE=$HOME/.bash_history; HISTFILESIZE=500; HISTSIZE=500	
DC4-C10-14	Los fallos deben ser registrados y analizados y se deben tomar las correspondientes acciones.	**Responsable**		**0**
	¿Quedan registrados los fallos reportados por los sistemas o los usuarios ?	Sí, el demonio syslogd (Syslog Daemon) se lanza automáticamente al arrancar un sistema Unix, y es el encargado de guardar informes sobre el funcionamiento de la máquina. Recibe mensajes de las diferentes partes del sistema (núcleo, programas...) y los envía y/o almacena en diferentes localizaciones.	/etc/syslog.conf	
	¿Esta información es analizada y son tomadas las acciones correspondientes?		Justificación: No se revisan los logs porque el encargado de revisarlo es el responsable de seguridad, y actualmente los logs no se cargan en Gales que es donde debe realizarse dicha revisión.	
DC4-C10-15	Los relojes de todos los sistemas de procesamiento de la información dentro de una Organización o de un dominio de seguridad, deben estar sincronizados con una precisión de tiempo acordada.	**Responsable**		**1**
	¿Está sincronizados los relojes de todos los sistemas de procesamiento?	Sí, los relojes están sincronizados con el servidor de dominio de comunitel.		

Figura 16. Ejemplo de cuestionario verificado

Todos los cuestionarios son cargados a la aplicación para que los datos puedan luego aparecer en los informes que automáticamente, y como veremos más adelante, se generarán

10.4.2 Scripts (Verificación/Carga en la Plataforma)

Con respecto a la verificación automática esta se lleva a cabo mediante un script que al ejecutarlo verifica el cumplimiento o no del control.

Para cada uno de los controles automáticos existe un scripts de verificación específico para cada tipo de sistema.

De igual manera, el resultado de una verificación solo puede tener dos estados:

- **Verificación satisfactoria**: El control se cumple.
- **Verificación no conforme**: El control no se cumple.

El repositorio de los resultados de la verificación de datos de cada ciclo ha de estar construidos sobre una BBDD u otro mecanismo que permita su explotación, seguimiento y generación de documentos de diagnóstico personalizados para obtener cualquier tipo de información mediante las consultas adecuadas.

10.5 Reporte – Generación de Informes

10.5.1 Generación y envío de Informes de no conformidades

Una vez cargadas las verificaciones en nuestra herramienta, se extraen las verificaciones no conformes, las cuales serán enviadas a los responsables para que las analicen, y corrijan, justifiquen o planifiquen.

Se realiza un informe por cada una de las aplicaciones verificadas, este informe es un fichero excel, que contiene una pestaña por cada una de las capas que le apliquen.

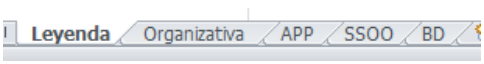


Figura 17. Ejemplo pestañas de Informe de No Conformidades

SUBCONTROL	DESCRIPCION	MÁS INFORMACION	RESULTADO	USUARIO	Comentarios/Justificación del	Responsable asignado	Fecha Planificada de	Estado
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	agarci10		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	banton		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	calonsot		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	cmartin5		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	crios		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	ebarber		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	fgonzal7		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	jdiaz3		ADMUyA		
DC5-C02-03	Las solicitudes de alta de usuarios se deben realizar a través de los procedimientos establecidos (P-0-0223 para ADM-UyA y N-0-0411 para IDM) siguiendo los flujos de aprobación definidos en	El usuario no tiene solicitud SASI asociada	No Conforme	jmartine		ADMUyA		

Figura 18. Ejemplo Informe de No Conformidades enviado al responsable.

Este fichero Excel debe ser completado por los responsables indicando su comentario o justificación, en el caso de que la no conformidad se planifique, también deberán incluir la fecha estimada de esta planificación.

10.5.2 Recepción y validación de Informes de NC.

Una vez recibidos los informes de no conformidades completados por los responsables, se procede a su validación, comprobando que las respuestas son coherentes.

Según los informes de no conformidades van siendo recepcionados, se revisa que estén completas cada una de las pestañas con sus respuestas correspondientes, estas respuestas deben estar acorde a las preguntas, en su defecto se volverá a contactar con el responsable para que complete las respuestas faltantes.

Si el informe esta completo con respuestas coherentes se procede a su validación.

SUBCONTROL	DESCRIPCION	MÁS INFORMACION	RESULTADO	USUARIO	Comentarios/Justificación del Responsable	Responsable asignado (login, tlf, departamento al que pertenece)	Fecha Planificada de Cambio	Estado
DC4-C01-01	Deben documentarse y mantenerse los procedimientos de operación y ponerse a	Comprobar cuestionario	No Conforme		Este control está siendo revisado por el responsable de ABALON	Responsable	2012-03-31 00:00:00.001	Planificada
DC4-C03-01	La utilización de los recursos se debe supervisar y ajustar, así como, realizar proyecciones de los requisitos futuros de capacidad, para garantizar el	Comprobar cuestionario	No Conforme		Este control está siendo revisado por el responsable de ABALON	Responsable	2012-03-31 00:00:00.001	Planificada
DC4-C03-02	Se deben establecer los criterios para la aceptación de nuevos sistemas de información, de las actualizaciones y de nuevas versiones de los mismos, y se deben llevar a cabo pruebas	Comprobar cuestionario	No Conforme		Este control está siendo revisado por el responsable de ABALON	Responsable	2012-03-31 00:00:00.001	Planificada
DC4-C05-02	Se deberán establecer procedimientos de actuación para la realización de copias de respaldo (al menos semanalmente), salvo que	Comprobar cuestionario	No Conforme		Este control está siendo revisado por el responsable de ABALON	Responsable	2012-03-31 00:00:00.001	Planificada
DC4-C05-03	Se deberán establecer procedimientos para la recuperación de los datos que garanticen en todo momento su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción. Para los ficheros o tratamientos parcialmente automatizados, y siempre que la existencia de documentación	Comprobar cuestionario	No Conforme		Este control está siendo revisado por el responsable de ABALON	Responsable	2012-03-31 00:00:00.001	Planificada
DC4-C05-04	El responsable del fichero se encargará de verificar cada seis meses la correcta definición, funcionamiento y aplicación de los	Comprobar cuestionario	No Conforme		Este control está siendo revisado por el responsable de ABALON	Responsable	2012-03-31 00:00:00.001	Planificada
DC4-C10-01	Los sistemas deben guardar un registro de los intentos de acceso correctos e incorrectos	Comprobar cuestionario	No Conforme		Este control está siendo revisado por el responsable de ABALON	Responsable	2012-03-31 00:00:00.001	Planificada
DC4-C10-02	Se deben realizar registros de auditoría de las actividades de los usuarios, las excepciones y eventos de seguridad de la información, y se deben mantener estos registros durante un período acordado para servir como prueba en	Comprobar cuestionario	No Conforme		Requeriría modificar el código de la aplicación y desde hace bastante tiempo no se realizan modificaciones de código ya que está prevista su desinstalación.	Responsable		Justificada

Figura 19. Ejemplo de Informe de No Conformidades con respuestas del responsable

10.6 Carga de justificaciones / planificaciones en la herramienta

Una vez que los informes están validados se les da el formato correspondiente para poderlos cargar en la aplicación.

Subcomponente	Subcontrol	tiposistem	diagnostico	resultado	parametr	valor	comentarioresponsable	fechaPlanificacio	estado
AIDA_ORG	DC1-C01-05	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Debido a la gran cantidad de contratos que se firman en VF-ES, los responsables y periodos de vigencia no son incluidos dentro del documento de seguridad, toda esta información es incluida en el contrato y esta declarada en la AGPD.		Justificada
AIDA_ORG	DC1-C01-08	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Se indica el cargo debido a la rotación de funciones.		Justificada
AIDA_ORG	DC4-C04-04	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información.	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC4-C06-04	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información.	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC4-C08-07	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Para los datos con nivel inferior a nivel alto no se utilizan soportes físicos para el movimiento de datos, se utilizan redes telemáticas.		Justificada
AIDA_ORG	DC4-C09-03	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información..	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC5-C04-03	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información..	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC5-C04-06	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información..	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC5-C04-16	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información..	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC5-C05-01	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Cumplimiento parcial de requisitos. (N-0-0445)		Justificada
AIDA_ORG	DC5-C06-05	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información..	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC6-C03-04	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información..	2012-03-31 00:00:00.001	Planificada
AIDA_ORG	DC8-C01-03	Organizativo	Comprobar cuestionario	No Conforme	NULL	NULL	Este control esta siendo revisado por Seguridad de la Información..	2012-03-31 00:00:00.001	Planificada

10.7 Generación de evidencias para informes de auditoría

Una vez que están cargados todos los datos en la aplicación, es decir todas las verificaciones con sus respuestas correspondientes, se procede a la generación de las carpetas y ficheros que servirán para mostrar las evidencias en el informe de auditoría. Para ello se utilizan dos procedimientos, el primero genera la ruta de las fichas técnicas, la ruta de las evidencias y las carpetas donde se guardaran los ficheros con las evidencias.

10.7.1 Generación de informes de auditoría

La generación de los informes de auditoría se lleva a cabo desde la herramienta

Figura 20. Imagen de la plataforma que muestra el menú desde el que se generan los informes de pre-auditoría

Es necesario seleccionar el marco normativo del que se desea generar el informe.

Figura 21. Imagen que muestra el menú del marco normativo sobre el que se quiere generar el informe

A continuación se elige la aplicación de la que se desea extraer el informe de auditoría y presionamos el botón "Informe de Auditoría".

Figura 22. Imagen donde se muestra como se elige la aplicación sobre la que se quiere generar el informe.

A continuación un extracto de un informe de auditoría:

CONTROL POLÍTICA SEGURIDAD

Fecha: 16/02/2012

2. VERIFICACIÓN DE CONTROLES CAPA SISTEMA OPERATIVO

Relación Normativas	Identificador SubControl	Descripción	Resultado	Tipo de Sistema
SOX - C9009 27002 - A 10.1 PCI DSS - 6.4	DC4-C01-09	Deben separarse los recursos de desarrollo, de pruebas y de operación, para reducir los riesgos de acceso no autorizado o los cambios en el sistema operativo.	Conforme	Solaris

Motivo o Evidencia

A continuación se muestra un extracto del cuestionario:

Pregunta	Respuesta	Comentario
¿Están separados los entornos de desarrollo, pruebas, y producción?	Sí, los entornos están separados. Los cambios en producción se realizan mediante peticiones PSR o SR. La herramienta de gestión de incidencias y planificaciones es Remedy 7.0.	

La Evidencia se encuentra en la siguiente ruta:

\\esm9-cips1\cps-sox\03_servicio\FY1112C2\00_poblaciones\AIDA\#Cuestionario_AIDA_FY1112C2_cargado.xls

Figura 23. imagen de informe de auditoría

10.8 Seguimiento de no conformidades planificadas

Entre la finalización de un ciclo y hasta la verificación de las no conformidades del siguiente ciclo, se lleva a cabo una revisión de las planificaciones existentes que tengan fecha de vencimiento comprendida en este intervalo. Se contacta con los responsables para o bien corregir estas no conformidades en los informes o bien cambiar la fecha de planificación si esta se ha demorado.

10.9 Mejora continua

Tras la finalización de un ciclo comienza la etapa de mejora, en esta etapa se subsanan los posibles errores que se hayan cometido durante el ciclo, (cuestionarios, scripts, procedimientos), y también se optimizan los distintos procesos ejecutados, o creando algunos nuevos para mejorar la calidad y precisión de los mismos.

Capítulo 11

Gestión del Proyecto

En este apartado se abordarán los aspectos más importantes que se han llevado a cabo para la consecución del proyecto, tales como la planificación realizada para la elaboración del documento, una valoración económica del mismo y las herramientas que se han empleado para poder elaborarlo.

11.1 Planificación del Proyecto

En esta sección se van a resumir las diferentes fases que se han ido produciendo hasta poder concluir este proyecto.

Fase 1: Análisis:

- **Objetivo del proyecto:** Determinar el objetivo principal del proyecto y los subobjetivos del mismo.
- **Alcance del proyecto**: Determinar la profundización en los diversos temas tratados, así como el alcance de los mismos.
- **Solución del proyecto**: Proponer y acordar una solución que aborde todos los objetivos a cumplir.

Fase 2: Planificación

- **Actividades necesarias:** Determinar todas las actividades que se han de realizar para ejecutar el proyecto.
- **Recursos disponibles**: Esclarecer qué recursos tanto humanos como técnicos se van a disponer para poder desarrollar el proyecto.

Fase 3: Desarrollo

- **Recopilación de información**: Una vez fijados los objetivos a cubrir, se ha de buscar todo tipo de documentación que pueda aportar información interesante y válida para el proyecto.
- **Selección de información:** De toda la información recogida, filtrar sólo la información más interesante y acorde a los objetivos del proyecto.
- **Elaboración de los contenidos**: Una vez acabado el proceso de documentación, se realiza la redacción de los contenidos del documento en base a los conocimientos adquiridos durante la documentación.
- **Revisión de los contenidos**: Toda vez que se ha confeccionado el documento, se pasa a revisar cada uno de los apartados para la aprobación final.

Fase 4: Entrega

- **Entrega del proyecto**: Una vez acabado y revisado, se procede a la entrega final del proyecto.

11.1.1 Estimación Inicial

En el momento en el que se inició el proyecto, se realizaron una serie de estimaciones relativas al coste económico que podía suponer la realización del mismo, y el tiempo que podía llevar completarlo.

Se estimó el 12 de Enero de 2015 como la fecha de inicio del proyecto, con un horario establecido de 18:00 a 22:00 de lunes a viernes (15 horas semanales), y con un precio estimado por cada hora de trabajo de 10€.

Con estos parámetros, se calcularon los días que se iban a dedicar a cada una de las tareas, como se ve reflejado en el siguiente cuadro:

Nombre de tarea	Duración	Comienzo	Fin
Proyecto Fin de Carrera	**176,2 días**	**lun 12/01/15**	**lun 15/06/15**
Fase 1: Análisis	**6,6 días**	**lun 12/01/15**	**vie 16/01/15**
Objetivos del Proyecto	0,8 días	lun 12/01/15	lun 12/01/15
Alcance del Poryecto	0,8 días	mar 13/01/15	mar 13/01/15
Solución del Proyecto	4 días	mié 14/01/15	vie 16/01/15
Fase 2: Planificación	**1,8 días**	**lun 19/01/15**	**mar 20/01/15**
Actividades necesarias	0,8 días	lun 19/01/15	lun 19/01/15
Recursos Disponibles	0,8 días	mar 20/01/15	mar 20/01/15
Fase 3: Desarrollo	**129 días**	**mié 21/01/15**	**jue 14/05/15**
Recopilación de Información	12 días	mié 21/01/15	vie 30/01/15
Selección de Información	15,2 días	lun 02/02/15	vie 13/02/15
Elaboración de los contenidos	87,2 días	vie 13/02/15	vie 01/05/15
Revisión de los contenidos	15,2 días	vie 01/05/15	jue 14/05/15
Fase 4: Entrega	**0,2 días**	**lun 15/06/15**	**lun 15/06/15**
Entrega delProyecto	0,8 días	lun 15/06/15	lun 15/06/15

Figura 24. Imagen de la estimación inicial de tiempo para llevar a cabo el PFC.

El resultado final era un proyecto con una duración estimada de 177 días, finalizando así el 15 de Junio de 2015. La dedicación por parte del alumno iba a ser del 100% en cada una de las tareas

El diagrama de Gantt que se obtuvo fue el siguiente:

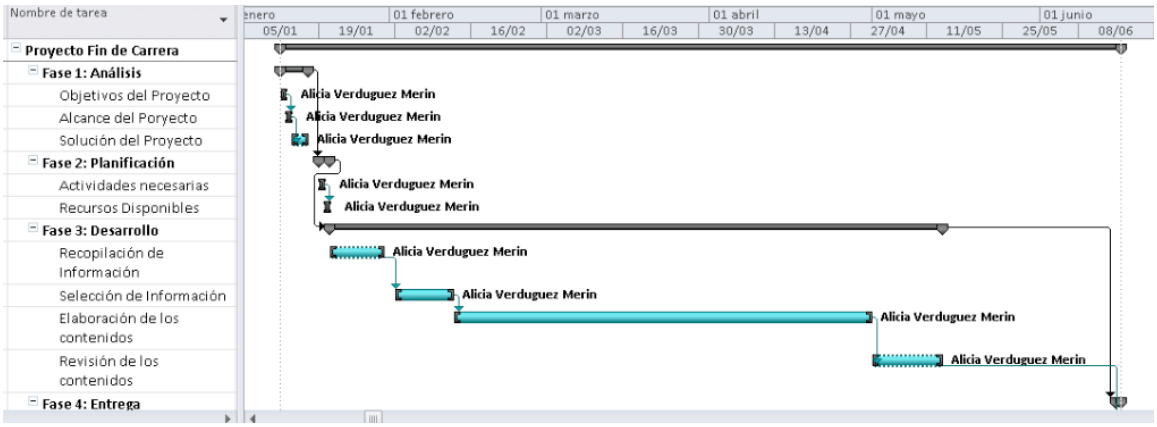


Figura 25. Diagrama de Gantt.

11.1.2 Planificación Real

Como ocurre en la mayoría de los proyectos, las expectativas no fueron cumplidas y los plazos fueron superados ampliamente, por lo que en este apartado se procede a reflejar los plazos que se cumplieron en realidad durante el desarrollo del proyecto.

Nombre de tarea	Duración	Comienzo	Fin
Proyecto Fin de Carrera	**301,6 días**	**lun 12/01/15**	**vie 02/10/15**
Fase 1: Análisis	**6,6 días**	**lun 12/01/15**	**vie 16/01/15**
Objetivos del Proyecto	0,8 días	lun 12/01/15	lun 12/01/15
Alcance del Poryecto	0,8 días	mar 13/01/15	mar 13/01/15
Solución del Proyecto	4 días	mié 14/01/15	vie 16/01/15
Fase 2: Planificación	**1,8 días**	**lun 19/01/15**	**mar 20/01/15**
Actividades necesarias	0,8 días	lun 19/01/15	lun 19/01/15
Recursos Disponibles	0,8 días	mar 20/01/15	mar 20/01/15
Fase 3: Desarrollo	**288,2 días**	**mié 21/01/15**	**mié 30/09/15**
Recopilación de Información	44 días	mié 21/01/15	vie 27/02/15
Selección de Información	34,4 días	lun 02/03/15	mar 31/03/15
Elaboración de los contenidos	204 días	mié 01/04/15	vie 25/09/15
Revisión de los contenidos	4 días	lun 28/09/15	mié 30/09/15
Fase 4: Entrega	**0,8 días**	**jue 01/10/15**	**vie 02/10/15**
Entrega delProyecto	0,8 días	jue 01/10/15	vie 02/10/15

Figura 26. Estimación real de tiempo para llevar a cabo el proyecto.

11.1.3 Análisis de la Planificación

Cabe mencionar que los costes calculados corresponden sólo a costes humanos, por lo que más adelante se comentará con más detalle los costes totales de la elaboración del proyecto.

Como se observa, existe una diferencia considerable entre lo estimado y lo que ha ocurrido finalmente (125 días). Esto es debido a que la realización del proyecto comenzó a alargarse y antes de concluirlo tuvo lugar el nacimiento de mi hija, lo cual hizo que se demorará aún más en el tiempo, y lo que tenía una fecha fin inicial del 30 de mayo se transformó en el 30 de septiembre, pues a partir del 21 de mayo fecha en que tuvo lugar dicho acontecimiento me resultaba bastante complicado en algunas ocasiones cumplir con los horarios establecidos.

Los meses de mayor bajón fueron junio, julio y agosto pues los avances en esos meses fueron muy escasos. En septiembre el horario se amplio, las horas dedicadas pasaron a ser 8 diarias de 9 a 13 horas de la mañana y de 15 a 19 de la tarde, sumando por tanto 176 horas de dedicación durante ese mes.

En cuanto al costo se observa un incremento final en torno a los 4.932€, ya que pasamos de un presupuesto inicial de 7.108€ a un presupuesto final de 12.040€. Donde no están computadas las horas extras llevadas a cabo en el mes de septiembre. Esto es

debido a que la duración final del proyecto ha sido mayor de la esperada, por lo que se han ido aumentando los costes al utilizar mayor tiempo los recursos disponibles.

11.2 Recursos empleados

En este apartado se mencionaran los recursos, materiales y humanos, empleados para el desarrollo del presente proyecto

RECURSO	TIPO	NOMBRE
HARDWARE	Ordenador Portátil	Apple MacBook
	Disco Duro Externo	Disco Duro Externo Portátil Tosiba 1Tb
	Impresora	Impresora HP Laser
SOFTWARE	Sistema Operativo	Mac OS X
	Navegador	Google Chrome Web Browser
	Procesador de Texto	Microsoft Office Word 2010
	Planificador y Gestor de Proyectos	Microsoft Office Project 2010
	Elaboración Diapositivas	Microsoft Office Power Point 2010
	Almacenamiento web	Disco web y dropbox

Tabla 7. Tabla de recursos empleados para la realización del PFC.

11.3 Balance Económico

A continuación se procederá a analizar los aspectos económicos derivados de la realización del proyecto. En este aspecto, se ha decidido clasificar los diferentes gastos dependiendo de su naturaleza, dividiéndolos en tres apartados:

- Costes Humanos: Derivados de las horas de dedicación de las personas que han participado en el desarrollo del proyecto.
- Costes Materiales: Derivados de todos los recursos materiales que se han usado para el desarrollo del proyecto.

- Otros costes: Cualquier otro gasto que no pudiera englobarse en ninguno de los dos apartados anteriores.

Primeramente, se verán los costes asociados a los recursos humanos:

PUESTO	COSTE/HORA	TOTAL HORAS	COSTE TOTAL
Alicia Verduguez Merin	10€	1.204	12.040 €

Tabla 8. Planificación real para costes humanos.

Ahora, los costes materiales:

DESCRIPCCIÓN	**COSTE (EUROS)**	**%Uso dedicado al proyecto**	**Dedicación (meses)**	**Periodo de depreciación**	**Coste total**
Ordenador Portátil	1000	100	9	48	187,61
Paquete Microsoft	140	100	9	48	26,25
Disco duro Externo	76,9	100	9	48	14,42

Tabla 9. Planificación real para costes materiales.

Costes acarrados por otro tipo de gastos:

TIPO	COSTE/HORA	TOTAL HORAS	COSTE TOTAL
Material de Oficina			40 €

Tabla 10. Planificación real para otro tipo de gastos.

Por último, se añaden a esos cálculos el 20% estimado como costes indirectos, calculado a partir de la suma de los costes materiales y el material de oficina, lo que supone 53,65 € más.

Finalmente, se procede a calcular la totalidad de costes acarreados durante el desarrollo del proyecto, según la planificación final:

Costes Humanos	6.020
Costes Materiales	228,28
Otros Costes	40
Costes Indirectos	53,65
TOTAL	6.341,93

Tabla 11. Total de costes.

Capítulo 12

Conclusiones Finales

En este apartado se abordarán los aspectos más importantes que se han llevado a cabo.

Primeramente, comentar que tras finalizar el documento, se puede concluir que la misión principal del mismo ha quedado resuelta, ya que este manual podrá servir a los usuarios como una guía de medidas a tener en cuenta para preservar la seguridad en los diferentes dispositivos que un usuario pueda disponer e incluso para poder percatarse de los peligros que esconde Internet y las técnicas que pueden emplear los delincuentes informáticos para poder perpetrar sus acciones.

A través de este documento, el usuario podrá extraer la información suficiente para protegerse en todo momento de cualquier amenaza que pueda atacar a su dispositivo informático y poder mantener fuera del alcance de los infractores los datos contenidos en estos.

Además, el lector podrá informarse acerca del marco legal actual en este aspecto de la informática,

Este documento alberga también el prototipo de una aplicación con vistas a la comercialización cuyo objetivo sea el de evaluar cuan de seguro es un dispositivo o aplicación. El capítulo abre un abanico de posibilidades bastante amplio sobre posibles nuevos proyectos a realizar. Así, puede suponer un comienzo para un estudio más en profundidad sobre el prototipo mencionado, otra alternativa sería un particularizarlo aún más en función de una determinada política o normativa.

CAPÍTULO 12: CONCLUSIONES FINALES

Para finalizar, pienso que este proyecto es bastante útil dado que ningún usuario es ajeno a las amenazas sobre la seguridad informática. Por muy experto o muy precavido que pueda llegar a ser un usuario, siempre van a aparecer nuevos mecanismos, nuevas formas de actuar con posibles consecuencias nefastas para nuestros equipos informáticos, por lo que considero de gran utilidad el transmitir mediante este documento, no sólo las posibles delitos o fraudes, sino las pautas a seguir para protegerse de ellos e incluso los derechos que el usuario pose

Referencias

[AEDP] *Agencia Española de Protección de Datos*
<http://www.agdp.es/portalwebAGDP/index-ides-idphp.php>

[ALEG] *Definición de Seguridad informática. Alegsa, Portal de Internet, informática y tecnologías de la información.*
<http://www.alegsa.com.ar/Dic/seguridad%20informatica.php>

[FIRDIG] *Firma Digital*.
<http://www.consumer.es/web/es/tecnologia/internet/2004/01/23/94524.php>

[ISO27001] *Estándar Internacional ISO 27001*. Disponible [Internet]
<http://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf >

[ISO27002] *Estándar Internacional ISO 27002.* Disponible [Internet]
< http://sgsi-iso27001.blogspot.com/2007/09/iso-27001-en-castellano.html>

[LOPD] *Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de carácter personal*.
<http://www.boe.es/aeboe/consultas/bases_datos/doc.php?id=BOE-A-1999- 23750>

[MODLOPD] *Modificación de la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de carácter personal.*
<http://marketingpositivo.blogspot.com/2011/03/entrada-en-vigor-de-la- reforma-de.html>

[RD1720] *REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de Diciembre, de protección de datos de carácter personal*.
http://www.boe.es/boe/dias/2008/01/19/pdfs/A04103-04136.pdf

[CPTRED] *Pagina web de seguridad*
http://www.criptored.upm.es/crypt4you/temas/privacidad-proteccion/leccion4/leccion4.html

[UC3MSEG].*Guia de seguridad de la Universidad Carlos III*
http://www.uc3m.es

[ENS] *Esquema nacional de seguridad*
http://administracionelectronica.gob.es/pae_Home/pae_Estrategias/pae_Seguridad_Inicio/pae_Esquema_Nacional_de_Seguridad.html#.VgvH4LTtmko